NAGASHIMA OHNO & TSUNEMATSU NY LLP
長島・大野・常松 法律事務所 ニューヨーク・オフィス

NO&T U.S. Law Update
米国最新法律情報

米国最新法律情報　2022 年 9 月　No.80
個人情報保護・データプライバシーニュースレター　2022 年 9 月　No.19

連邦プライバシー法案の公表

弁護士 逵本 麻佑子
弁護士 長谷川 紘

はじめに

2022 年 6 月 3 日、米国連邦データプライバシー保護法（the American Data Privacy and Protection Act）の法案（以下、「本法案」といいます。）が連邦議会超党派議員により公表されました。本法案は、長年におよぶ連邦議会の超党派による議論の上立案された連邦法上のデータプライバシー保護に係る法案であり、2022 年 6 月 23 日に連邦議会下院におけるエネルギー・商業委員会（U.S. House Committee on Energy and Commerce）の審議に付されました [1]。米国においては、カリフォルニア州消費者プライバシー法（the California Consumer Privacy Act[2]（以下、「CCPA」といいます。））、バージニア州消費者データ保護法（the Virginia Consumer Data Protection Act（以下、「CDPA」といいます。））、コロラド州プライバシー法（the Colorado Privacy Act（以下、「CPA」といいます。））及びユタ州消費者プライバシー法（the Utah Consumer Privacy Act（以下、「UCPA」といいます。））のように、一部の州において個別の個人情報保護法が制定されてきましたが、本法案は、連邦法として初めてとなる包括的な個人情報保護法の法案です。本法案の規定は、これらの州法の規定と同様の規律を含む一方、連邦法特有の規定も多分に含み、また、本法案はこれらの州法に原則として優先して適用される（州法は preempt される）こととされています。本法案が法として成立した場合、実務に与える影響は大きいものと考えられ、本ニュースレターでは、本法案の概要及び従前の州法との主な相違点を紹介します [3]。

本法案の概要

1. 適用範囲

(1) 適用される者の範囲

対象エンティティ

本法案は以下 a.又は b.に該当する者を対象エンティティ（covered entity）と定義し [4]、対象データ

[1] https://energycommerce.house.gov/newsroom/press-releases/pallone-opening-remarks-at-subcommittee-markup-of-bipartisan-bicameral
https://energycommerce.house.gov/sites/democrats.energycommerce.house.gov/files/documents/BILLS-117hr8152ih.pdf

[2] 2020 年 11 月 3 日に成立したカリフォルニア州プライバシー権法（the California Privacy Rights Act（以下、「CPRA」といいます。））は、CCPA の改正及び追加的規制を定めており、2023 年 1 月 1 日付で施行される予定です。

[3] 本ニュースレターにおいて紹介する本法案の内容は 2022 年 8 月 19 日時点のものを前提としており、今後の立法の過程で内容に変更があり得ます。

[4] Section 2(9)。なお、政府機関や政府のために対象データを取得、処理又は移転する者は除外されています。

（covered data）（定義につき下記(3)をご参照ください。）の処理に関して一定の義務を課しています。

a. 次の①及び②の要件を満たす者
   ① 対象データの収集、処理（process）[5]又は移転（transfer）の目的及び手段を、単独で又は第三者と共同で決定する者（非商業目的で行為する個人を除く。）であり、かつ
   ② (i)連邦公正取引委員会法（the Federal Trade Commission Act）[6]の適用を受ける者[7]、(ii)1934年通信法（the Communications Act of 1934）第2節（title II）[8]の適用を受ける通信事業者（common carrier）又は(iii)自らの又は自らの構成員の利益のために事業を行うために組成されたものではない組織（organization）
b. 他の対象エンティティを支配する者、他の対象エンティティにより支配される者、又は他の対象エンティティと共同の支配下にある者

大規模データ保有者

本法案は、次の a.及び b.記載の要件に該当する対象エンティティを大規模データ保有者（large data holder）と定義し[9]、対象データの処理に関して追加の義務（詳細については下記 3. 以下をご参照ください。）を課しています。

a. 直近の歴年において、総収益（annual gross revenue）が$250,000,000 以上であり、かつ、
b. 直近の歴年において、次の①又は②のいずれかの対象データを収集し、処理し又は移転する者。但し、(i)私用 E メールアドレス、(ii)私用電話番号又は(iii)対象エンティティによって管理されるアカウントへのログインに必要となる個人又はデバイスのログイン情報の収集又は処理によってのみ該当する場合を除く。
   ① 5,000,000 名超の個人又は 5,000,000 個超の所定のデバイス[10]（1 名以上の個人を識別するデバイス又は 1 名以上の個人とリンクされた若しくは合理的にリンク可能なデバイス。以下同様。）の対象データ
   ② 200,000 名超の個人又は 200,000 個超の所定のデバイスのセンシティブ対象データ[11]。

小規模対象エンティティ

一方で、本法案は、対象エンティティのうち、次の要件に該当する小規模のものについては、一部の義務[12]の適用を除外しています[13]。

直近の 3 年間（対象エンティティが 3 年以上存続していない場合においては、対象エンティティが存続した期間）において、次の a.、b.及び c.の要件を満たすこと。

a. 当該期間における平均の年間総収益が$41,000,000 を超えないこと。
b. 当該期間において、対象エンティティが、平均して、1 年間で 200,000 名超の個人の対象データを、要求されたサービス又は商品の開始、提供、請求、確定、完了又は代金回収の目的（ただし、これらの目的のためのすべての対象データが 90 日以内に削除又は非識別化（de-identified）される場合に限る。）以外の目的で収集し又は処理していないこと。
c. 当該期間中のいずれかの年（対象エンティティの設立が 1 年未満の場合は、その年の一部）において、対象エンティティが対象データの移転によって収益の 50%超を得ていないこと。

---

[5] Section 2(19)において、対象データの分析、整理、構造化、保持、使用又はその他の取扱いを含む、対象データに対して行われるあらゆる操作又は一連の操作を意味すると定義されています。

[6] 15 U.S.C. 41 et seq.

[7] 連邦公正取引委員会法（the Federal Trade Commission Act）の適用を受ける者の範囲については、脚注 64 をご参照ください。

[8] 47 U.S.C. 201-231

[9] Section 2(17)

[10] Section 2(12)において、「デバイス」とは、対象となるデータの送受信が可能な電子機器であって、個人が使用するために設計されたものと定義されています。

[11] センシティブ対象データの定義については、脚注 28 をご参照ください。

[12] 対象データの移転請求に応じる義務（Section 203(a)(4)）、データ・セキュリティ・プラクティスを確立する義務の一部（Section 208(b)(1)-(3) and (5)-(7)）及びプライバシー・オフィサー/データ・セキュリティ・オフィサーの選任義務（Section 301(c)）。

[13] Section 209(a)

(2) 個人の範囲

本法案は、保護の対象となる個人（individual）について、米国に居住する自然人と幅広く定義しています[14]。

(3) 対象データの範囲

本法案によって保護される対象データ（covered data）は、単体で又はその他の情報と合わせて、(i)個人若しくは(ii)所定のデバイスを識別する情報、又は、上記(i)若しくは(ii)とリンクされた若しくは合理的にリンク可能な情報をいい、派生データ（derived data）[15]及び一意の識別子（unique identifiers）[16]を含むと定義されています[17]。そして、対象データは、非識別化されたデータ（de-identified data）[18]、従業員データ（employee data）[19]、公開情報（publicly available information）、又は複数の独立した公開情報（個人に関するセンシティブ対象データを明らかにするものを除く。）の情報源のみから作成された推論（inferences）を含まないとされています。ここでいう公開情報とは、対象エンティティが以下の①、②、③、④又は⑤の情報源から適法に公共に提供されていると信じるにつき合理的な理由がある情報と定義されています[20]。

① 連邦、州又は地方政府機関の記録（但し、対象エンティティが、関連する政府機関によって付された制限又は使用条件を遵守して当該情報を収集し、処理し、移転する場合に限る。）
② 広く頒布されたメディア
③ 全ての公衆に対して有償又は無償で提供されるウェブサイト又はオンラインサービス（全ての公衆が当該ウェブサイト又はオンラインサービスにログインすることで利用できる場合を含む。）
④ 連邦、州又は地方政府機関の求めにより一般公衆に開示されたもの
⑤ 公共の場における個人の物理的存在に係る外観観察（当該個人の保有するデバイスによって収集されるデータを含まない。）

2. 消費者の権利

本法案では、個人の権利として、主に以下の権利が規定されています[21]。

- 以下の情報へのアクセス権：
  ① 過去 24 ヶ月間に、対象エンティティ又は対象エンティティのサービス・プロバイダによって収集、処理又は移転された個人の対象データ（バックアップ又はアーカイブシステムにあるものを除く。

[14] Section 2(16)

[15] Section 2(11)において、個人やデバイスに係る事実、証拠又はその他の情報源若しくはデータから、情報、データ、仮定又は結論を派生させることによって作成された対象データを意味すると定義されています。

[16] Section 2(35)において、個人、又は、1 名以上の個人を識別し若しくは 1 名以上の個人とリンクされた若しくは合理的にリンク可能なデバイスに、合理的にリンク可能な識別子を意味し、デバイス識別子、インターネットプロトコルアドレス、クッキー、ビーコン、ピクセルタグ、モバイル広告識別子又は同様の技術、顧客番号、固有の仮名若しくはユーザーエイリアス、電話番号、その他の個人又はデバイスとリンクされ又は合理的にリンク可能な永続的又は確率的な識別子を含むとされています。

[17] Section 2(8)

[18] Section 2(10)において、非識別化されたデータ（de-identified data）とは、情報が集積されている場合であるか否かを問わず、個人を識別しない又は個人とリンクしない若しくは合理的にリンク可能ではない情報又はデバイスと定義されています。当該非識別化されたデータに該当するためには、対象エンティティが、(i)いかなる場合においても、当該データが、個人又はデバイスが再度識別される形で用いられないことを確実にするための合理的な措置を実施し、(ii)情報を再度識別する合理的な手法のない非識別化された様式で処理し移転すること及び再び個人又はデバイスの情報を識別する試みをしないことを公にコミットし、かつ、(iii)情報の受領者に対して上記事項を遵守することを契約上義務付けることが必要となります（Section 2(10)）。

[19] Section 2(8)(C)において、大要、従業員候補者の情報、従業員の連絡先、緊急連絡先又はベネフィットの管理等（administering benefits）に必要な範囲で収集し、処理し又は移転する情報とされています。

[20] Section 2(23)。もっとも、同条において、公開情報には以下の情報は含まれないとされています。(i)わいせつ表現、(ii)複数の独立した公開情報（個人に関するセンシティブ対象データを明らかにするものを除く。）の情報源のみから作成された推論（inferences）、(iii)バイオメトリクス情報、(iv)対象データと組み合わされた公開情報、(v)遺伝子情報（genetic information）及び(vi)意に反すると知られているプライベート画像（known nonconsensual intimate images）。

[21] Section 203(a)

合理的な個人であれば内容が理解可能で、インターネットからダウンロード可能な、読解可能な（human-readable）形式による。）

② 対象エンティティが個人の対象データを有償で移転した先の第三者の名称及びサービス･プロバイダのカテゴリー、並びに対象データが収集された情報源のカテゴリー

③ 対象エンティティが第三者、他の対象エンティティ又はサービス･プロバイダに対して個人の対象データを移転した目的

- 訂正権：対象エンティティによって処理される個人の対象データについて、重大な不正確性又は重大な点において不完全な情報を訂正し、対象エンティティが当該対象データを移転した第三者、他の対象エンティティ又はサービス･プロバイダに対して訂正した情報を通知させる権利
- 削除権：対象エンティティによって処理される個人の対象データを削除し、対象エンティティが当該対象データを移転した第三者、他の対象エンティティ又はサービス･プロバイダに対して、当該個人による削除要請を通知させる権利
- データポータビリティ権：技術的に可能な範囲において、対象エンティティによって処理される個人の対象データ（派生データを除く。）を、当該移転を制限するライセンス制限なしに、個人又は他のエンティティに直接移転（export）する権利（(i)合理的な個人であれば内容が理解可能であり、インターネットからダウンロード可能で読解可能な形式かつ、(ii)ポータブルで、構造化され、相互運用可能で機械による読み取り可能な形式による。）

上記権利を行使された場合、対象エンティティは、原則として 60 日以内に対応する必要がありますが、対象エンティティが大規模データ保有者に該当する場合は 45 日以内に対応する必要がある一方で、小規模対象エンティティに該当する場合は、90 日以内に対応することで足りることとされています [22]。

更に、上記の権利に加え、本法案では、個人の権利として、対象データの移転及びターゲティング広告からのオプト・アウトを求める権利が定められています [23]。

3. 対象エンティティの義務

本法案は、対象エンティティに対して、対象データの処理に関する以下の義務を課しています。

(1) データの最小化（Data Minimization）

- 対象エンティティは、以下の①、②又は③のいずれかの目的のために合理的に必要かつ相応な（proportionate）範囲 [24]を超えて、対象データを収集、処理又は移転してはならないとされています [25]。
  ① 個人によって求められた具体的な商品若しくはサービス提供若しくは維持のため
  ② 対象エンティティと個人との間の関係の中で合理的に予期される、対象エンティティから当該個人へなされるコミュニケーションの提供若しくは維持のため
  ③ 本法案において明示的に許諾されている目的 [26]のため

(2) 忠実義務（禁止行為）

- 本法案において、対象エンティティは、本法案に記載の所定の例外を除き、以下の行為を行うことが原則として禁止されます [27]。
  ① 社会保障番号の収集、処理又は移転
  ② センシティブ対象データ [28]の収集及び処理（当該収集若しくは処理が、当該センシティブ対象デ

[22] Section 203(c)

[23] Section 204(b)、(c)

[24] 今後ガイダンスが出される予定です（Section 101(c)）。

[25] Section 101

[26] 例えば、個人から具体的に求められた取引を開始し若しくは完了し、又は個人から具体的に求められた注文若しくはサービスを実行する場合や、セキュリティ事故の予防、特定、セキュリティ事故からの保護又はセキュリティ事故への対応等の目的を含む、12 の例外となる目的が列挙されています（Section 101(b)）。

[27] Section 102

[28] Section 2(24)において、以下に該当する対象データを指すものと定義されています。(i)ソーシャルセキュリティナンバー、パスポートナンバー、運転免許証ナンバー等の公に表示することが想定されていない政府が発行する識別子、(ii)個人の過去、現在又は将来の

ータに係る個人によって求められた特定の商品若しくはサービスの提供若しくは維持、又は、本法案において明示的に許諾されている目的のために、厳密に必要となる場合を除く。）

③ センシティブ対象データの第三者への提供（当該個人による積極的かつ明示的な同意がある場合、連邦法又は州法に基づき課された義務の順守に必要となる場合等の本法案において明示的に認められている例外を除く。）

④ 個人の集約されたインターネットの検索履歴又はブラウジング履歴の収集、処理又は移転

(3) 内部規程の策定義務

- 本法案において、対象エンティティには、その事業の規模、性質、範囲及び複雑性、問題となる個人データの機微性及び量、問題となる個人又はデバイスの量、導入コスト等を考慮し、対象データの収集、処理及び移転について、大要、以下を目的とする合理的なポリシー、プラクティス及び手続を設定する義務が課されています[29]。

① 対象エンティティが収集、処理又は移転する対象データに関する連邦、州又は地方の法、規則及び規制の考慮

② 17 歳未満の個人についてのプライバシー・リスクの低減等

③ 対象エンティティの商品及びサービス（これらのデザイン、開発及び運用を含む。）についてのプライバシー・リスクの低減

④ 対象エンティティが、又はサービス･プロバイダが対象エンティティのために、収集、処理又は移転する対象データに適用のある全てのプライバシー法令の遵守を促進し、又はプライバシー・リスクを低減させるための、対象エンティティ及びサービス･プロバイダ内における合理的なトレーニング及び安全措置（safeguards）の実施

(4) 価格決定等に関する個人への忠実義務（条件付けの禁止）

- 対象エンティティは、法又は法に基づき公布される諸規則において認められたプライバシー権の放棄の有無により、サービス又は商品の個人への提供を拒否したり、条件付けたり又は実質的に条件付けることや、このようなプライバシー権を放棄することを拒絶したことをもって、個人に対してサービスを停止し又はサービス若しくは商品の提供を拒絶することが禁止されます[30]。

(5) プライバシー・ポリシーの公表義務及びプライバシー・ノーティス義務

- 本法案において、対象エンティティは、対象データの収集、処理及び移転活動に関する詳細かつ正確な表現を提供するプライバシー・ポリシーを、明確で見やすく、容易にアクセス可能な方法で、一般に公開することが義務付けられます[31]。プライバシー・ポリシーの内容は以下の内容を最低限含むこととされてい

身体の健康状態、精神の健康状態、障害、治療若しくは診断に係る情報、(iii)金融口座番号、デビットカード番号、クレジットカード番号又は収入レベル若しくは銀行口座残高に関する情報、(iv)生体情報、(v)遺伝子情報、(vi)正確な地理的位置情報、(vii)ボイスメール、電子メール、テキスト、ダイレクトメッセージ、郵便物などの個人の私的なコミュニケーション、又はそのコミュニケーションの当事者を特定する情報、音声コミュニケーション、電話番号、通話元の電話番号、通話時間、通信当事者の位置情報などの音声コミュニケーションの送信に関するあらゆる情報（対象エンティティが発信者又は意図した受信者でない場合に限る。）、(viii)アカウント又はデバイスのログイン資格情報又はセキュリティ・アクセス・コード、(ix)個人の性的指向又は性的活動を、当該個人の合理的な期待に反する方法で特定する情報、(x)カレンダー情報、アドレス帳情報、電話若しくはテキストログ、写真、オーディオ録音、又は個人のデバイスで私的使用のために維持されるビデオ（これらの情報が別の場所にバックアップされているかどうかにかかわらない。）、(xi)個人の裸又は下着姿の私的領域を写した写真、フィルム、ビデオ録画、又はその他類似の媒体、(xii)放送テレビサービス、ケーブルサービス、衛星サービス又はストリーミングメディアサービスのプロバイダに個人が要求又は選択したビデオコンテンツ又はサービスを明らかにする情報、(xiii)17 歳未満の個人の情報、(xiv)上記の類型のデータを特定する目的で収集され、処理され又は移転されたその他の対象データ。

[29] Section 103。今後ガイダンスが出される予定です（Section 103(c)）。

[30] Section 104(a)。もっとも、対象エンティティが、個人による対象エンティティとの継続的な取引と引き換えに、割引又は無料の商品若しくはサービス又はその他の対価を提供するロイヤルティ・プログラムを提供することは禁止されないなど、所定の例外があります（104(b)）。

[31] Section 202

ます。

① 対象エンティティの情報と連絡先（プライバシー及びデータ・セキュリティに関する問い合わせにかかる対象エンティティの連絡先、一般的なＥメールアドレス及び電話番号を含む。）及び対象エンティティによって対象データが移転される対象エンティティと同一の企業ストラクチャー内にある他のエンティティの情報と連絡先
② 対象エンティティが収集又は処理する対象データのカテゴリー
③ 当該カテゴリーの対象データを収集又は処理する目的
④ 対象エンティティによる対象データの移転の有無。移転を行う場合、(i)対象エンティティが対象データを移転する先のサービス･プロバイダ及び第三者のカテゴリー、(ii)対象エンティティが対象データを移転する第三者収集エンティティ（定義につき下記 4.をご参照ください。）の各名称、並びに(iii)当該データが当該カテゴリーのサービス･プロバイダ及び第三者又は第三者収集エンティティに移転される目的
⑤ センシティブ対象データを含む、対象データのカテゴリー毎の保存期間。当該期間を特定することができない場合は、当該カテゴリーの対象データの保存期間を決定するために用いられる基準。
⑥ 個人の権利の行使方法
⑦ 対象エンティティによるデータ・セキュリティ・プラクティスの一般的な記述
⑧ プライバシー・ポリシーの施行日
⑨ 対象エンティティが収集した対象データが中国、ロシア、イラン又は北朝鮮に移転され、これらの国で処理若しくは保存され、又はその他の方法で利用可能とされているか否か

- プライバシー・ポリシーについて重大な変更がある場合、対象エンティティは、従前収集された対象データの更なる処理又は移転がなされる前に、当該重大な変更によって影響を受ける各個人に対して通知を行う義務を負い、所定の例外に該当する場合を除き、各個人に対して、変更後のポリシーにおける対象データの更なる収集、処理又は移転についての同意を撤回するための合理的な機会を提供することが求められます [32]。
- プライバシー・ポリシーに加えて、大規模データ保有者は、対象データについて、以下の内容及び様式の通知を行う義務を負うこととされています [33]。

① 簡単、明確かつ明瞭であること（concise, clear, and conspicuous）
② 個人が当該大規模データ保有者及びその商品又はサービスと交流（interact）する方法並びに個人との関係性において合理的に予期される方法に照らして、容易にアクセス可能であること
③ 個人の権利の概要が含まれており、また、合理的に予期しない方法でなされ得るデータ・プラクティスやセンシティブ対象データに関わるデータ・プラクティスについて合理的に注意を喚起する方法で開示されること
④ 500 文字以内であること

(6) 対象データの移転制限/ターゲット広告に関する制限

- 本法案は、対象データの移転について、以下の制限を設けています。

① 当該個人が拒否する場合には、（センシティブ対象データに限らず、）個人の対象データを第三者に移転してはならず、法 [34]の制定から 18 ヶ月以内に連邦取引委員会（Federal Trade Commission、以下「FTC」といいます。）により構築される所定の統一オプト・アウトメカニズムに基づくオプト・アウトを許諾しなければならない [35]。
② 対象エンティティは、知れている 17 歳未満の個人について、当該個人、当該個人の親又は保護者の積極的な明示的同意なくして、個人の対象データを第三者に移転してはならない [36]。

- また、ターゲット広告について、本法案は以下の制限を設けています。

[32] Section 202(e)
[33] Section 202(f)
[34] 米国連邦データプライバシー保護法を指します。以下同様です。
[35] Section 204(b)、Section 210
[36] Section 205(b)

① ターゲット広告を行う対象エンティティは、ターゲット広告を行う前及び行った後、個人に対してターゲット広告からオプト・アウトするための明確かつ明瞭な方法を提供しなければならず、個人がオプト・アウト要請を行った場合、これに従う義務を負う。また、この際のオプト・アウトについては、対象エンティティは、所定の統一オプト・アウトメカニズムに基づくオプト・アウトを許諾しなければならない [37]。

② 対象エンティティは、知れている 17 歳未満の子どもにつき、ターゲット広告を行ってはならない [38]。

(7) 差別的取扱いの禁止/データアルゴリズムに関する影響評価

- 対象エンティティは、人種、肌の色（color）、宗教、国籍（national origin）、性別又は障害に基づき、差別的な方法で、又は商品若しくはサービスの平等な享受をできなくする方法で、対象データを収集し、処理し、又は移転してはならないとされています [39]。
- 更に、本法案は、「アルゴリズム」を「機械学習、自然言語処理、人工知能技術又はこれらと同等以上の複雑性を有するその他の計算処理技術を用いた計算処理であって、対象データに関する決定を行い又は人間の意思決定を促進するもの（商品若しくはサービスの提供の決定、又は個人への情報の配信若しくは表示のランク付け、順序付け、促進、推奨、増幅、若しくは決定のためのものを含む。）」と定義し [40]、アルゴリズムを使用又は開発する一定の対象エンティティに対して、以下のアセスメント又は評価の実施義務を課しています [41]。

① 対象データの収集、処理又は移転の全部又は一部についてアルゴリズムを使用している大規模データ保有者は、法の制定から 2 年以内、またその後毎年、当該アルゴリズムの影響について所定のアセスメントを実施しなければならない。

② 対象データの収集、処理又は移転のためのアルゴリズムを知りながら開発する対象エンティティは、法の制定から 2 年以内に、当該アルゴリズムのデザイン（アルゴリズムを開発するために用いられたトレーニング・データを含む。）の評価を行わなければならない。

上記の適用を受ける対象エンティティは、上記のアセスメントを FTC に提出する義務を負い、更に、連邦議会の求めがある場合、連邦議会に対して提出することが求められています。

(8) 安全管理措置

- 対象エンティティは、対象データを不正なアクセス及び取得から保護するために、合理的な管理上、技術上及び物理上のデータ・セキュリティ・プラクティス及び手続を確立し、実施し、維持する義務を負います [42]。当該合理的な管理上、技術上及び物理上のデータ・セキュリティ・プラクティスは、(i)対象エンティティの規模及び複雑性、(ii)対象エンティティによる対象データの収集、処理又は移転の性質及び範囲、(iii)収集、処理又は移転される対象データの量及び性質、(iv)収集、処理又は移転される対象データの機微性、(v)対象データを保護するための管理上、技術上又は物理上のセーフガードの最新の状況、並びに(vi)対象データのリスクと性質に関連して、当該対象データのセキュリティを向上させ、不正アクセスや不正取得に対する脆弱性を低減するために利用可能なツールのコスト、を考慮することが求められます。
- 更に、本法案は、当該データ・セキュリティ・プラクティスにおいて最低限含まれるべき事項として、以下の事項を掲げています [43]。

(i) 脆弱性評価

対象データの収集、処理又は移転を行う対象エンティティが維持する各システムのセキュリティに対する内部及び外部の重大なリスク及び脆弱性を特定し評価すること。これには、当該対象データ

[37] Section 204(c)
[38] Section 205(a)
[39] Section 207(a)
[40] Section 2(2)
[41] Section 207(c)
[42] Section 208(a)
[43] Section 208(b)

への不正アクセス又はリスク、人的脆弱性、アクセス権、及びサービス･プロバイダの利用が含まれる（任意の団体又は個人による脆弱性の未承諾の報告を受け、これに対応するための計画も含まれる。）。

(ii) 防止措置及び是正措置

対象エンティティが特定した対象データに対する合理的に予見可能なリスク又は脆弱性を軽減するための予防措置及び是正措置を採ること（管理上、技術上又は物理上の保護手段の導入、データ・セキュリティ慣行若しくは構成の変更、又はネットワーク若しくはオペレーティング・ソフトウェアのインストール若しくは実装を含む。）。

(iii) 予防措置及び是正措置の評価

技術上の重大な変化、対象データに対する内部又は外部の脅威、及び対象エンティティ自身の事業体制又は運営の変化に照らして、上記(ii)に記載されたセーフガードを評価し、合理的に調整を加えること。

(iv) 情報の保持と処分

法律で削除が義務付けられている対象データ又は収集、処理若しくは移転の目的に照らし必要ではなくなった対象データの処分（ただし、個人が当該データの保持に積極的に同意した場合は、この限りではない。）。

(v) トレーニング

対象データにアクセスする各従業員に対し、対象データの保護方法に関するトレーニングを実施し、必要に応じて当該トレーニングを更新すること。

(vi) 役員等の選任

上記のデータ・セキュリティ・プラクティスを維持し、実施するための役員又は従業員を選任すること。

(vii) インシデント対応

セキュリティ事故・違反の検出、対応、回復のための手順を実施すること。

(9) プライバシー・オフィサー等の選任義務

- 本法案において、対象エンティティは、次の a.及び b.のオフィサーをそれぞれ選任する義務を負うこととされています[44]。
  a. 1 名以上のプライバシー・オフィサー
  b. 1 名以上のデータ・セキュリティ・オフィサー
- これらのオフィサーは、(i)本法案の要件に従い、対象データのプライバシー及びセキュリティを保護するためのデータ・プライバシー・プログラム及びデータ・セキュリティ・プログラムを実施し、(ii)対象エンティティによる本法案の遵守を促進することが求められます。
- 更に、上記 a.及び b.に加えて、大規模データ保有者は、下記(10)記載のプライバシー保護責任者を選任する義務を負うこととされています[45]。

(10) 大規模データ保有者による証明書の提出義務

- 法の制定から 1 年後以降、大規模データ保有者の執行役員（executive officer）は、毎年 FTC に対して以下の事項を記載した証明書（certificate）を提出する義務を負うこととされています[46]。当該証明書は、提出 90 日前までに証明を行う役員により実施された大規模データ保有者の内部統制及び報告構造の有効性のレビューに基づく必要があります[47]。
  ① 法を遵守するために合理的な内部統制が維持されていること
  ② 証明書を提出する役員が、当該対象エンティティによる法の遵守に影響を与える決定について関

[44] Section 301(c)
[45] Section 301(c)(3)
[46] Section 301(a)
[47] Section 301(b)

与し、責任を有することを確保するための報告制度が維持されていること

- 更に、大規模データ保有者は、証明書を提出する役員のうち少なくとも 1 名を、当該大規模データ保有者の最高責任者に直接報告するプライバシー保護責任者として任命しなければならないとしています [48]。当該責任者は、上記(9)記載の義務に加え、次のことを行う義務を負います。
  - ① 必要に応じて、大規模データ保有者のプライバシー及びセキュリティに関するポリシー、慣行及び手続を定期的に見直し、更新するためのプロセスを確立すること
  - ② 適用されるすべての法律を遵守していることを確認するために、大規模データ保有者の業務のポリシー、慣行、手順が機能していることを確保するための包括的な監査を隔年で実施し、FTC が当該監査についてアクセスできることを確保すること
  - ③ 遵守要件について従業員を教育・訓練するプログラムを開発すること
  - ④ 大規模データ保有者が行った全てのプライバシー及びデータ・セキュリティ施策について、最新の（updated）、正確で、明確かつ理解しやすい記録を維持すること
  - ⑤ 大規模データ保有者と執行当局との間の連絡窓口となること

(11) 大規模データ保有者によるプライバシー影響評価

- 法の制定から 1 年以内又は対象エンティティが大規模データ保有者の定義を満たした日から 1 年以内のいずれか早い日及びその後 2 年ごとに、各大規模データ保有者は、大規模データ保有者の対象データの収集、処理及び移転の実務によって得られた利益（benefit）と当該実務が個人のプライバシーに潜在的に与え得た悪影響を比較検討する所定のプライバシー影響評価を行う義務が課されています [49]。

4. 第三者収集エンティティ（third-party collecting entities）の義務

本法案は、所定の例外を除き、対象データに係る個人から直接収集したわけではない個人の対象データの処理又は移転を主な収入源としている対象エンティティを、第三者収集エンティティ（third-party collecting entity）と定義し [50]、第三者収集エンティティに対して、自らが第三者収集エンティティである旨を個人に対して所定の方法で通知する義務を課し、また、5,000 名以上の個人又は 5,000 個以上のデバイスに係る対象データを処理することとなった場合に、翌年の 1 月 31 日までに FTC に対して登録する義務を課しています [51]。

5. サービス･プロバイダ及び第三者の義務

本法案は、所定の内容を含む書面による契約に基づき対象データを対象エンティティから又は対象エンティティのために受領し、対象エンティティのために、かつ、その指示に基づき、対象データを収集、処理又は移転する対象エンティティを、サービス･プロバイダ（service provider）と定義し [52]、サービス･プロバイダに対して、通常の対象エンティティの義務に加え、以下の義務を課しています [53]。

- 対象エンティティから要求されたサービスの提供のために合理的に必要な範囲及び相応な（proportionate）範囲に限り、対象データを収集し、処理し移転する義務
- 対象エンティティがあるデータについて法に違反したと実際に知っている場合には、当該対象データを収集し、処理し又は移転してはならない義務
- 対象エンティティが個人の権利行使に応じる義務を充足するために、対象エンティティを、適切な技術的及び組織的な措置により支援する義務
- 更に他のサービス･プロバイダを使用する場合には、対象エンティティに事前に通知し、かつ、当該他のサービス･プロバイダに対して自らと同等の義務を課す内容の書面による契約書を締結する義務
- 対象エンティティの要請があった場合、法に基づく自らの義務の遵守を示す必要な情報を提供する義務

[48] Section 301(c)(3)
[49] Section 301(d)
[50] Section 2(32)
[51] Section 206
[52] Section 2(25)
[53] Section 302(a)

- 法令に基づく例外を除き、対象エンティティの指示のもと、サービス終了時に対象データを消去し又は返還する義務
- 当該個人と直接的な関係を有する対象エンティティによって個人の積極的な同意が取得されることなくして、サービス･プロバイダが保有するデータを、他のサービス･プロバイダを除く第三者に移転しない義務
- 対象データのセキュリティ及び機密性を確保するため、合理的な管理上、技術上及び物理上のセーフガードを確立し、実施し、維持する義務

更に、本法案は、所定の例外を除き、対象エンティティにより移転された対象データを収集し、処理し又は移転する者であり、かつ、当該データについてサービス･プロバイダに該当しない者を第三者（third party）と定義し[54]、原則として通常の対象エンティティの義務を負うことを明記するほか、対象エンティティが公表した目的以外の目的（センシティブ対象データの場合は当該個人が積極的かつ明示的に同意した目的以外の目的）のために、対象データを処理しない義務を課しています[55]。加えて、対象エンティティは(i)サービス･プロバイダの選任及び(ii)第三者への対象データへの移転を決定するに際しては、合理的な調査（due diligence）を実施する義務を負うこととされています[56]。

6. 法に違反した場合の制裁

法の違反は、連邦公正取引委員会法における不当又は詐欺的な行為又は慣行（unfair or deceptive act or practice）の防止に係る規定の違反に該当するものとみなされ[57]、FTC は、同法に基づき差止命令等の規制権限[58]を行使する権限を有するほか、法に違反した対象エンティティに対する民事救済（契約の取消若しくは変更、金銭の払戻し、損害賠償の支払い、公表等）を求めて提訴する権限を有することとされています[59]。

また、FTC に加え、各州の司法長官（attorney general of a State）又は各州のプライバシー当局（State Privacy Authority）は、法又は法に基づく規則に違反した対象エンティティに対して、行為の差止め、法又は法に基づく規則の遵守の履行強制、損害賠償の請求、民事罰の請求、利益の返還請求その他の補償の請求、合理的に生じた弁護士費用及び訴訟費用の請求を求めて連邦裁判所に提訴する権限を有することとされています[60]。

更に、本法案は、私的訴権についても明示的に認めています。施行日から 4 年後以降、法又は法に基づく規則の違反により損害を被った個人は、連邦裁判所に対して所定の損害賠償請求、差止命令請求、確認請求、合理的に生じた弁護士費用及び訴訟費用の請求訴訟を提起することが可能とされています[61]。当該私的訴権については、請求が差止命令の請求の場合、又は、所定の小規模対象エンティティに対する請求の場合には、45 日前の通知と是正期間が設けられています[62]。また、私的訴権を行使する場合、本法案は、FTC と自らが居住する州の司法長官に、このような訴訟を提起する旨を事前に通知しなければならないとしており、これらの機関は、当該個人に代わり訴訟を提起するか否かを 60 日以内に判断しなければならないとしています[63]。

---

[54] Section 2(31)
[55] Section 302(d)
[56] Section 302(c)
[57] Section 401(c)(1)
[58] 15 U.S.C. 45(b)
[59] 15 U.S. Code § 57b。もっとも、懲罰的損害賠償の請求は認められていません（15 U.S. Code § 57b(b)）。
[60] Section 402(a)
[61] Section 403(a)
[62] Section 403(c)
[63] Section 403(a)(3)(A)

本法案の特徴・影響

1. 対象エンティティの範囲

CCPA、CDPA、CPA 及び UCPA のような、従前の州法レベルにおいては、対象となる事業者に該当する要件として、いずれも個人情報の取扱量が一定の基準に達していること又は一定の事業規模があることが求められていました。一方で、本法案においては、このような個人情報の取扱量や事業規模を対象エンティティ該当性の要件とはしておらず、上記の通り、対象データを収集し、処理し又は移転する者である場合、対象エンティティとして法の適用の対象となり得る点で適用範囲が広範であると考えられます[64]。また、本法案では、他の対象エンティティを支配する者等についても、本法案上の「対象エンティティ」に該当するとされていますので、日系企業の米国子会社が本法案上の「対象エンティティ」の要件を満たせば、日本の親会社も本法案の適用を受ける可能性があります[65]。

また、従前の州法では、適用の対象となる事業者を区分し、区分毎に規制内容を変えるということは行われていませんでしたが、本法案は、大規模データ保有者又は小規模対象エンティティに該当する場合、個別の規制内容が異なる点でも特徴的です。特に大規模データ保有者に該当する場合には、上記の通り、所定の証明書の提出、プライバシー保護責任者の選任、プライバシー影響評価の実施といった追加的な義務を負うなど、従前の州法より負担の重い規制が設けられているという特徴があります。

2. 対象データの範囲

従前の州法においては、保護される個人データ又は個人情報について、いずれも公開情報をその定義から除外しており、本法案も公開情報を対象データから除外していますが、公開情報の定義の内容には差異があります。すなわち、CCPA では、公開情報とは、連邦政府、州政府又は地方政府の記録から適法に入手可能な情報を意味すると定義されていますが、本法案では、CDPA 及び UCPA と同様に、これらの情報に加えて、「広く頒布されたメディア」（widely distributed media）を通じて一般大衆に適法に入手可能となった情報も含まれます。

更に、本法案は、CPA で規定されているのと同様、統一オプト・アウトメカニズムを用いたオプト・アウトを認める規定がある点で特徴的です。

3. センシティブ対象データの取扱い

本法案においては、センシティブ対象データに、従前の州法でセンシティブ・データに含まれていたような、個人の人種、民族起源、国籍、宗教的信条、労働組合の組合員であることの有無が含まれていません。一方で、一部の州法と同様に個人の特定位置情報はセンシティブ対象データに含まれています。

センシティブ・データの取扱いについて、一部の州法においては、消費者の同意までは求められていないケースもありますが、本法案は、CDPA 及び CPA と同様に、センシティブ対象データの処理について個人の同意を必要としており、より対象データの保護に積極的な規制枠組みになっています[66]。

---

[64] 対象エンティティ該当性の要件としては、上記の通り、対象データを収集し、処理し又は移転する者であることの他に、連邦公正取引委員会法（the Federal Trade Commission Act）の適用を受ける者等の制限がありますが、同法は、本法案にも関係する不当又は詐欺的な行為又は慣行（unfair or deceptive act or practice）との関係では商取引（commerce）に従事する全ての者に適用されるとする FTC のマニュアルがあり（https://www.federalreserve.gov/boarddocs/supmanual/cch/200806/ftca.pdf）、この点を前提とすると、対象エンティティの範囲は広範に及ぶ可能性があります。

[65] CDPA、CPA 及び UCPA においてはこのようなグループ会社にもその適用を拡大する規定はありませんが、CCPA においては、同様に CCPA の要件を満たす事業者を支配し又は当該事業者により支配される者で、当該事業者とブランドを共通にする主体についても、CCPA 上の「事業者」に該当するとされています。

[66] UCPA においては、センシティブ・データの処理の際には、消費者に対する明確な通知及びオプト・アウトの機会の提供が求められていますが、消費者の同意までは求められておりません。CCPA においても、CPRA によって、事業者がセンシティブ個人情報を収集する場合は、収集するセンシティブ個人情報のカテゴリー、利用目的等を消費者に提供しなければならず、消費者は、事業者に対して、

4. エンフォースメント

従前の州法においては、CCPA において私的訴権が認められている一方、CDPA、CPA 及び UCPA では私的訴権が明文で否定されていました。本法案は、CCPA と同様に一定の範囲で個人に私的訴権を認めており、CDPA、CPA 及び UCPA より個人の保護が厚くなっています。

5. その他対象エンティティの義務の範囲

上記の他、本法案においては、対象エンティティに対して、具体的な内部規程の策定義務やプライバシー・ポリシーの作成及び公表義務を設けるなど、ガバナンス体制のあり方について様々な義務を課しています。従前の州法でも、所定のプライバシー・ノーティスを行う義務や、所定の安全管理措置を講じる義務等が事業者には課されていましたが、本法案においては、1 名以上のプライバシー・オフィサー及び 1 名以上のデータ・セキュリティ・オフィサーを選任する義務が定められ、特に大規模データ保有者についてはこれらに加えてプライバシー保護責任者の選任等、州法レベルでは見受けられない様々なガバナンスへの規制が課されています。また、対象データについて、アルゴリズムを使用する一部の対象エンティティについては、一定のアセスメントの実施が義務付けられるなど、従前の州法では規定されていなかった AI 技術に対する個人データの取扱いへの監督も強化されています。

6. 州法との関係

本法案においては、いかなる州又は州の政治的下部組織も、所定の例外を除き、法又は法に基づき公表される規則、ルール若しくは要件によって管轄される事項について、法的な効力を有する法律、規制、ルール等を採用し、維持し、実施し、又は効力を継続してはならないとされており、原則として、法は州法に優先して適用されるものとされています[67]。本法案は、例外として州法が法に優先する場合の類型を限定的に列挙していますが[68]、具体的にどの範囲で州法が独自に適用されるかについては必ずしも明らかではなく、今後の動向を注視する必要があります。

今後に向けて

本法案は、制定から 180 日後に施行されることとされていますが、具体的な制定見込み時期は明らかとなっていません。本法案は 2022 年 6 月に公表されましたが、今後控えている米国中間選挙の影響もあり、今期の国会において十分に審議する時間の確保が難しいほか、私的訴権や他の州法への優越に関する規定といった、議論を呼び得る条項が含まれていることに鑑みると、本法案について直ちに米国議会のコンセンサスが得られる見込みは低いとの見立てもあります。いずれにしても、本法案は上記の通り事業者に対して非常に広範かつ詳細な規制を課そうとするものであり、実務に重大な影響をもたらすため、今後の審議の過程を注視する必要があります。

2022 年 9 月 1 日

センシティブ個人情報の利用を一定の場面に限定することを求めることができることとされていますが、消費者の同意が求められていないという点で UCPA と類似しています。

[67] Section 404(b)。

[68] 所定の例外として、主に以下のものが列挙されています。(i)消費者保護法、(ii)市民権法、(iii)従業員、従業員情報、学生、又は学生情報のプライバシー権又はその他の保護について定めた法律、(iv)情報漏えい時の通知義務に関する法律、(v)契約法、不法行為法、(vi)詐欺等に関する刑事法、(vii)サイバー・ストーキング等に係る刑事・民事法、(viii)プライバシー又はセキュリティと無関係な公共安全に関する法律、(ix)刑事訴訟記録等に関する法律、(x)信用情報等の記録に関する法律、(xi)顔面認識テクノロジー等に関する法律、(xii)イリノイ州における生体情報プライバシー保護法（740 ILCS 14 et seq.）及び遺伝情報保護法（410 ILCS 513 et seq.）、(xiii)迷惑メール、電話勧誘等に関する法律、(xiv)保健記録等に関する法律、(xv)図書記録の秘密に関する法律、(xvi)カリフォルニア州民法 Section 1798.150。情報漏えい時の通知義務に関しては多くの州で個別の法律が制定されているところ、上記の通り、これらの法律については依然各州法の定めが適用されるため、情報漏えいが生じた際には、引き続き州毎の個別の対応の検討が必要となります。

[執筆者]

塗本 麻佑子（Nagashima Ohno & Tsunematsu NY LLP 弁護士 パートナー）
mayuko_tsujimoto@noandt.com
2008 年京都大学法学部卒業。2016 年 Harvard Law School 卒業（LL.M.）。2010 年弁護士登録（第一東京弁護士会）、長島・大野・常松法律事務所入所。2016 年より長島・大野・常松法律事務所ニューヨーク・オフィス（Nagashima Ohno & Tsunematsu NY LLP）勤務。
入所以来、M&A を中心とした案件に従事し、近時はニューヨークを拠点として、日本及び米国のクライアントに対して企業法務全般にわたるリーガルサービスを提供している。

長谷川 紘（長島・大野・常松法律事務所 弁護士）
hiroshi_hasegawa@noandt.com
2011 年東京大学法学部卒業。2020 年 Harvard Law School 卒業（LL.M.）。2013 年弁護士登録（第一東京弁護士会）、長島・大野・常松法律事務所入所。2020 年 9 月から 2022 年 8 月まで長島・大野・常松法律事務所ニューヨーク・オフィス（Nagashima Ohno & Tsunematsu NY LLP）勤務。
入所以来、ファイナンス取引等を中心とした案件に従事し、国内外のクライアントに対して企業法務全般に関するリーガルサービスを提供している。

[編集者]

鈴木 明美　長島・大野・常松法律事務所 弁護士 パートナー
akemi_suzuki@noandt.com

森 大樹　長島・大野・常松法律事務所 弁護士 パートナー
oki_mori@noandt.com

殿村 桂司　長島・大野・常松法律事務所 弁護士 パートナー
keiji_tonomura@noandt.com

www.noandt.com

NAGASHIMA OHNO & TSUNEMATSU NY LLP

450 Lexington Avenue, Suite 3700
New York, NY 10017, U.S.A.
Tel: +1-212-258-3333（代表） Fax: +1-212-957-3939（代表） Email: info-ny@noandt.com

Nagashima Ohno & Tsunematsu NY LLP は、米国における紛争対応や日米間の国際取引について効率的な助言を行うことを目的に、長島・大野・常松法律事務所のニューヨーク・オフィスの事業主体として 2010 年 9 月 1 日に開設されました。米国の法務事情について精緻な情報収集を行いつつ、米国やその周辺地域で法律問題に直面する日本企業に対して、良質かつ効率的なサービスを提供しています。

長島･大野･常松 法律事務所

〒100-7036　東京都千代田区丸の内二丁目 7 番 2 号　ＪＰタワー
Tel: 03-6889-7000（代表） Fax: 03-6889-8000（代表） Email: info@noandt.com

長島・大野・常松法律事務所は、500 名を超える弁護士が所属する日本有数の総合法律事務所であり、東京、ニューヨーク、シンガポール、バンコク、ホーチミン、ハノイ及び上海にオフィスを構えています。企業法務におけるあらゆる分野のリーガルサービスをワンストップで提供し、国内案件及び国際案件の双方に豊富な経験と実績を有しています。