AMED説明文書用モデル文案
別紙「米国における個人情報の保護に関する制度に関する情報等」
（詳細版）

目次

第1　連邦法

1　個人情報の保護に関する制度の有無

個人情報保護に関する包括的な法令は存在しない[1]。個別の分野に適用される法令のうち代表的なものは、以下のとおりである。

なお、医療情報に関しては、医療保険の携行性と責任に関する法律（Health Insurance Portability and Accounting Act）の適用が主に想定される。また、特に、医療情報に関連する企業活動との関係において、連邦取引委員会法（Federal Trade Commission Act of 1914）は、消費者プライバシー保護に関する規制を行う根拠となりうる。

これら以外の連邦法についても、連邦レベルでの米国における個人情報保護制度の概要を理解するために有益であるため、合わせて説明を行うものである。

(1) 医療保険の携行性と責任に関する法律（Health Insurance Portability and Accounting Act、以下、「HIPPA」という。）

ア　URL[2]

https://www.cdc.gov/phlp/publications/topic/hipaa.html
（1996 年 8 月 21 日施行）

イ　対象となる情報

HIPAA は、プライバシー規則において、その保護対象を、「保護されるべき健康情報（Protected Health Information）」（健康状態、医療の提供、医療費の支払いに関連する情報で、個人を識別することでき、かつ、個人を特定できると信じるに足る合理的な根拠があるもの）[3]としている。

ウ　義務の対象者

HIPPA 上の義務の対象者は、公的機関（地方自治体を含む。）及び民間機関（①医療機関、医療供給者、健康計画（health plans）、②医療情報センター（health care clearinghouses）、③アメリカ合衆国保健福祉省（HHS）が採用した基準の対象となる処理に関連して全ての医療情報を電子送信する医療提供者[4]）である。

---

[1] 2022 年 6 月 3 日、包括的な個人情報保護法として American Data Privacy and Protection Act の法案（https://www.congress.gov/bill/117th-congress/house-bill/8152/text）が公表されたが、現時点（2023 年 6 月 23 日時点）において具体的な成立の見込みは不明である。

[2] 2023 年 6 月 23 日閲覧時点でのリンクである。

[3] 42 U.S.C. §17921., 45 CFR 160.103.

[4] 42 U.S.C. §17921., 45 CFR 160.103.

エ　義務及び禁止事項等

HIPPA に基づく「プライバシー規則」[5]及び「セキュリティ規則」[6]を遵守することが義務付けられる。

「プライバシー規則」は、健康情報の保護の国家基準を設定するものであり、①プライバシー規則により許可、又は、要求される場合、②対象となる個人（又は代諾者）が文書により許可した場合以外の場合において、保護されるべき健康情報を使用、開示してはならないとする[7]。使用、開示が許可される場合は、①個人に対するものである場合、②治療、支払い、又は医療業務を遂行するための使用及び開示の場合、③保護されるべき健康情報を保護するために、適切な管理的、技術的、及び物理的な保護措置を講じる等の条件を遵守していることを前提にした偶発的な使用及び開示の場合、④別途禁止される場合を除き、研究目的等で認可を得た場合、⑤個人に対して使用又は開示について事前に通知し、使用又は開示に同意し、又は使用若しくは開示を禁止若しくは制限する機会を与えた場合、⑥その他、法令により許可された場合、である[8]。開示が要求される場合は、個人（又は代諾者）が自分に関する健康情報へアクセスや開示を求めた場合[9]、及び、遵守状況確認調査又は措置実施の評価のために、保健社会福祉省（DHHS）に提供する場合[10]である。さらに、保護されるべき健康情報を使用若しくは開示する場合、又は保護されるべき健康情報を他の保護対象事業体若しくは業務関係者に要求する場合、保護対象事業体又は業務関係者は、保護されるべき健康情報を、使用、開示、又は要求の意図された目的を達成するために必要な最小限のものに限定するために合理的な努力を払わなければならないとされている[11]。

セキュリティ規則は、電子的に保持・移動される健康情報のセキュリティに関する国家基準を設定するものであり、対象事業者に対し、作成、受領、維持、又は送信するすべての電子的な保護されるべき医療情報の機密性、完全性、及び可用性を確保すること、当該情報のセキュリティ又は完全性に対する合理的に予想される脅威又は危険から保護すること、プライバシー規則上、許可又は要求されていない、当該情報の合理的に予想される使用又は開示から保護すること、従業員がコンプライアンスを遵守することを義務付けている[12]。具体的な保護措置として、管理上の保護措置（リスク分析やリスク管理の実施、セキュリティ担当者の特定、情報アクセス管理、従業員に対するセキュリティ意識向上とトレーニン

---

5 45 CFR 160, 45 CFR 164.102 - 164.106, 45 CFR164.500 - 164.534.
6 45 CFR 160, 45 CFR 164.102 - 164.106, 45 CFR 164.302 - 164.318.
7 45 CFR 164.502(a).
8 45 CFR 164.502(a)(1).
9 45 CFR 164.502(a)(2)(i), 45 CFR 164.524(a), 45 CFR 164.528(a).
10 45 CFR 164.502(a)(2)(ii).
11 45 CFR 164.502(b).
12 45 CFR 164.306(a).

グの実施等）[13]、物理的保護措置（施設のアクセス管理、執務スペースの物理的な保護、デバイス及びメディアの管理等）[14]、技術的保護措置（アクセスの制御、ユーザー識別等）[15]を規定している。

(2) 連邦取引委員会法（Federal Trade Commission Act of 1914）（以下「FTC 法」という。）

FTC 法 5 条は、「商業活動に関わる不公正な競争手段と、商業活動に関わる不公正又は欺瞞的な行為又は慣行は、違法である」[16]と規定しており、連邦取引委員会（Federal Trade Commission（FTC））が消費者プライバシー保護に関する規制を行う根拠となっている。

ア URL[2]

https://www.ftc.gov/legal-library/browse/statutes/federal-trade-commission-act
（1914 年 9 月 26 日施行）

イ 対象となる個人情報

以下のとおりである。

- 「特定の消費者、コンピュータその他の機器に合理的に結び付けることのできるデータ」（consumer data that can be reasonably linked to a specific consumer, computer, or other device）[17]
- 生体情報（Biometric Information）（識別された、又は識別可能な個人の身体に関する、物理的、生物学的、又は行動の特徴、特性、又は測定値を描写又は記述するデータ）[18]

ウ 義務の対象者

FTC 法上の義務の対象者は、民間機関である。

エ 義務及び禁止事項等

---

[13] 45 CFR 164.308.
[14] 45 CFR 164.310.
[15] 45 CFR 164.312.
[16] 15 U.S.C. § 45(a)(1).
[17] FTC, *FTC Report: Protecting Consumer Privacy in an Era of Rapid Change*, (Mar, 2012), https://www.ftc.gov/sites/default/files/documents/reports/federal-trade-commission-report-protecting-consumer-privacy-era-rapid-change-recommendations/120326privacyreport.pdf
[18] 連邦取引委員会（FTC）は、2023 年 5 月 18 日、「生体情報と FTC 法第 5 条に関する政策声明」（PolicyStatement）を発表し、生体情報または生体情報を利用した技術の FTC 法第 5 条の違反の可能性を評価する際に考慮しうる事情を非網羅的に列挙している。FTC, *Policy Statement of the Federal Trade Commission on Biometric Information and Section 5 of the Federal Trade Commission Act*, (May, 2024), https://www.ftc.gov/system/files/ftc_gov/pdf/p225402biometricpolicystatement.pdf

商業活動に関わる不公正な競争手段と、商業活動に関わる不公正又は欺瞞的な行為又は慣行を禁止しており、FTC 法は本条文を企業のプライバシー及びセキュリティデータ保護ポリシーを規制するために用いている。

FTC 法は、生体情報を収集・利用する企業、生体情報技術を利用する企業が FTC 法第 5 条を遵守しているかどうかを判断する際には、以下のような行為が違反の可能性があると判断することを示している。

① 生体情報を利用した技術の有効性、信頼性、正確性、性能、公正性、有効性に関する虚偽又は根拠のないマーケティング上の主張。
② 生体情報の収集と使用に関する欺瞞的な記述。
③ 生体情報を収集する前に、消費者に予見可能な損害を評価しなかったこと。
④ 既知又は予見可能なリスクへの迅速な対処を怠ること。
⑤ 生体情報を密かに、かつ予期せぬ形で収集又は利用すること。
⑥ 第三者の慣行や能力を評価しないこと。
⑦ 生体情報又は技術に接する従業員及び請負業者に対して、適切なトレーニングを提供しないこと。
⑧ 事業者が開発し、販売に供し、又は生体情報に関連して使用する技術について、継続的なモニタリングを実施しないこと。

(3) 電子通信プライバシー法（Electronic Communications Privacy Act of 1986）（以下「ECPA」という。）

ア URL[2]

https://bja.ojp.gov/program/it/privacy-civil-liberties/authorities/statutes/1285
（1986 年 10 月 21 日施行）

イ 対象となる個人情報

以下のとおりである。

- **有線通信**
  州際・国際的な通信、又は、州際若しくは国際商取引に影響を及ぼす通信のための施設の提供・運営に従事する者によって設置・運営された、電話線、ケーブル、又は、元の場所と受領する場所をつなぐもの（交換局のそのようなコネクションの使用を含む）による、通信のための機材を全般にわたり又は一部でも使用した音声の移転[19]。
- **口頭の通信**

[19] 18 U.S.C. §2510(1).

傍受がされないことを正当に期待し得る状況下において、傍受されないことの期待を示す者によってなされる口頭の通信。但し、電子通信は含まない[20]。

- **電子通信**

  州際又は国際商取引に影響を及ぼす有線、無線、電磁気、光電子又は写真光学システムによって、全部又は一部が送信された性質のサイン、シグナル、書面、画像、音、データ。但し、①有線又は口頭の通信、②音のみの呼出装置を通じた通信、③追跡装置を使用した通信、④電子的な保管場所やファンドの移転のために使用される通信システムにおいて、金融機関によって保管された情報を移転する電子ファンドは含まない[21]。

ウ　義務の対象者

ECPA 上の義務の主な対象者は、個人データの電子的保存[22]を行う公的機関（地方自治体を含む。）及び民間機関、である。

エ　義務及び禁止事項等

ECPA の第 1 章である通信傍受法（Wiretap Act）は、主に、法定の例外事由に該当する場合を除き、①有線通信、口頭の通信並びに電子通信を故意に傍受すること、及び、②法律違反を犯して傍受した情報であることを知っている場合、又は、このことを知る理由を有している場合、当該情報を利用、開示することを禁止している[23]。

また、ECPA の第 2 章である通信保存法（Stored Communications Act、SCA）は、①権限なくして（又は権限を超えて）、電子通信サービスのために利用されるシステムへアクセスすること、及び、それにより、そのシステムに保存されている有線通信又は電子通信への許可されたアクセスを取得、改ざん、又は妨害することを禁止している[24]。

ECPA の第 3 章は、政府の代理人弁護士（Attorney for the government）や国家捜査官又は法執行官（State investigative or law enforcement officer）に対し、電話利用状況記録装置又はトラップ＆トレース装置の設置及び利用については、その設置及び利用権限を与える裁判所の授権を取得することを義務付けている[25]。

---

[20] 18 U.S.C. §2510(2).

[21] 18 U.S.C. §2510(12).

[22] 「電子的保存」とは、電子的な送信に付随する通信の一時的、中間的な保存、及びバックアップ保護を目的とした電子通信サービスによる当該通信の保存を指す（18 U.S.C. §2511.）。

[23] 18 U.S.C. §2511(1).

[24] 18 U.S.C. §2701(a).

[25] 18 U.S.C. §3123(a).

(4) 児童オンラインプライバシー保護法（Children's Online Privacy Protection Act of 1998）（以下、「COPPA」という。）

ア　URL[2]

https://www.ftc.gov/legal-library/browse/rules/childrens-online-privacy-protection-rule-coppa
（2000 年 4 月 21 日施行）

イ　対象となる個人情報

COPPA の対象は、「特定の個人を識別可能なオンラインで収集された個人に関する情報」（氏名、 住所、オンライン上の連絡先情報、ウェブサイトやオンラインサービスを通じてユーザーを認識するために用いることのできる永続識別子、児童の画像又は音声が含まれる写真、映像又は音声ファイル、正確な地理位置情報その他収集され、これら要素のいずれかと共に組み合わされた情報を含む。）[26]である。

ウ　義務の対象者

COPPA 上の義務の対象者は、民間機関（ウェブサイト又はオンラインサービスを運営し、当該ウェブサイト又はオンラインサービスの利用者若しくは訪問者から個人情報を収集又は保持する者等 [27]）である。

エ　義務及び禁止事項等

ウェブサイト又はオンラインサービスにおいて、13 歳未満児童から収集する情報の内容、当該情報の利用方法、及び当該情報の開示方法について通知すること[28]、子供からの個人情報の収集、使用、及び/又は開示に先立ち、検証可能な親の同意を得ること [29]、親が子供から収集した個人情報を確認し、それ以上の使用又は維持を許可しないための合理的な手段を提供すること [30]、ゲーム、賞品の提供、又はその他の活動への参加を、当該活動への参加に合理的に必要な以上の個人情報の開示を条件としないこと [31]、及び、子どもから収集した個人情報の機密性、安全性、完全性を保護するための合理的な手順を確立し維持すること [32]を義務付けている。

---

[26] 16 CFR 312.2
[27] 16 CFR 312.2
[28] 16 CFR 312.4(b).
[29] 16 CFR 312.5.
[30] 16 CFR 312.6.
[31] 16 CFR312.7.
[32] 16 CFR312.8.

(5) グラム・リーチ・ブライリー法（Gramm Leach Bliley Act）（以下「GLBA」という。）

ア　URL[2]

https://www.ftc.gov/business-guidance/privacy-security/gramm-leach-bliley-act
（1999 年 11 月 12 日施行）

イ　対象となる個人情報

GLBA の対象は、「非公開個人情報」（①消費者から金融機関に対して提供され、②消費者との間の取引若しくは消費者のために履行されたサービスの結果又は③金融機関により別途取得されたもの）[33]である。

ウ　義務の対象者

GLBA 上の義務の主な対象者は、金融サービス業に「実質的に従事する（significantly engaged）」民間の金融機関、である。

エ　義務及び禁止事項等

GLBA は「セーフガード規則」を設けており、顧客情報を保護するために設計された管理的、技術的、物理的なセーフガードを備えた情報セキュリティプログラムを策定し、実施し、維持することを義務付けている[34]。また、プライバシー保護の運用基準を設けてこれを顧客に通知する等の「プライバシー規則」（Privacy Rule）を遵守することを義務付けている。これは「副題 A：非公開個人情報の開示」（Subtitle A: Disclosure of Nonpublic Personal Information）[35]において成文化された。

2　個人情報の保護に関する制度についての指標となり得る情報

(1) EU の十分性認定 [36]

---

[33] 15 U.S.C, §6809.

[34] 15 U.S.C. §6801(b), 6805(b)(2), 16 CFR 314.1. FTC, FTC Safeguards Rule: What Your Business Needs to Know, https://www.ftc.gov/business-guidance/resources/ftc-safeguards-rule-what-your-business-needs-know

[35] 15 U.S.C. §6801–6809.

[36] EU の十分性認定を取得した国又は地域は、個人情報保護委員会が日本と同等の保護水準にあると認められる個人情報の保護に関する制度を有する外国等として指定している EU（EU 加盟国及び欧州経済領域（EEA）の一部であるアイスランド、ノルウェー、リヒテンシュタイン）の個人情報の保護に関する制度である GDPR 又はその前身のデータ保護指令に基づき、欧州委員会が十分なデータ保護の水準を有していると認められる旨の決定を行っている国又は地域であることから、概ね日本と同等の個人情報の保護が期待できる。このような意味にお

現時点において、米国と EU 間では十分性認定はなされていない[37]。

(2) APEC の CBPR システム[38]

米国は、2012 年 7 月 25 日付で、APEC による CBPR システムへの参加を認められている[39]。

3 OECD プライバシーガイドライン 8 原則

(1) 民間部門

米国は APEC の CBPR システム参加エコノミーであるから、民間部門については、外国にある第三者に対する個人データの提供に伴うリスクについての本人の予測可能性は一定程度担保されると考えられる。

(2) 公的部門

公的部門に関し、OECD プライバシーガイドライン 8 原則に対応する公的部門の主体の義務又は本人の権利については、①収集制限の原則：HIPAA に一部規定されている、②データ内容の原則：該当する規定は見当たらない、③目的明確化の原則：該当する規定は見当たらない、④利用制限の原則：ECPA 及び HIPAA に一部規定、⑤安全保護の原則：HIPAA に一部規定、⑥公開の原則：該当する規定は見当たらない、⑦個人参加の原則：HIPAA に一部規定、⑧責任の原則：該当する規定は見当たらない、である。

4 その他本人の権利利益に重大な影響を及ぼす可能性のある制度

いて、EU の十分性認定を取得した国又は地域であることは、「個人情報の保護に関する制度についての指標となり得る情報」に該当する。

[37] なお、2022 年 12 月 13 日、欧州委員会が、EU-U.S. Data Privacy Framework に定められた個人データの保護に関する諸原則に準拠した個人データの処理を行う米国の事業者への個人データの移転に関する十分性認定のドラフト（https://commission.europa.eu/system/files/2022-12/Draft%20adequacy%20decision%20on%20EU-US%20Data%20Privacy%20Framework_0.pdf）を公表し、採択に向けた検討が進められている（https://ec.europa.eu/commission/presscorner/detail/en/ip_22_7631）。

[38] APEC の CBPR システム参加の前提として、APEC のプライバシーフレームワークに準拠した法令を有していること、及び CBPR 認証を受けた事業者やアカウンタビリティエージェントにおいて解決できない苦情・問題が生じた場合に執行機関が調査・是正する権限を有していること等が規定されていることから、我が国と同じく APEC の CBPR システムに参加しているエコノミーにおいては、APEC のプライバシーフレームワークに準拠した法令と当該法令を執行する執行機関を有していると考えられるため、個人情報の保護について概ね我が国と同等の保護が期待できる。このような意味において、APEC の CBPR システム参加エコノミーであることは、「個人情報の保護に関する制度についての指標となり得る情報」に該当する。なお、APEC の CBPR システムの対象は、民間部門である。

[39] Federal Trade Commission, *FTC Becomes First Enforcement Authority in APEC Cross-Border Privacy Rules System*, (last visited Jun 12, 2023), https://www.ftc.gov/news-events/news/press-releases/2012/07/ftc-becomes-first-enforcement-authority-apec-cross-border-privacy-rules-system

(1) 個人情報の域内保存義務に係る制度であって、本人の権利利益に重大な影響を及ぼす可能性のあるもの

この点を明示する制度は見当たらないである。

(2) 事業者に対し政府の情報収集活動への協力義務を課す制度であって、本人の権利利益に重大な影響を及ぼす可能性のあるもの

この点を明示する制度は見当たらないである。

第2　カリフォルニア州法

1　個人情報の保護に関する制度の有無

カリフォルニア州には、2023 年 6 月現在において、包括的な個人情報保護法としてカリフォルニア州消費者プライバシー法 （California Consumer Privacy Act、以下「CCPA」という。）を改正して成立したカリフォルニア州プライバシー権法（California Privacy Rights Act）が存在する。それに加えて、規制対象となるデータの種類（健康情報等）によって、その取扱いを個別に規制する州法が存在する。カリフォルニア州法上の主なプライバシー規定は、以下のとおりである。

(1) カリフォルニア州プライバシー権法（California Privacy Rights Act、以下「CPRA」という。）

ア　URL[2]

https://www.oag.ca.gov/system/files/initiatives/pdfs/19-0021A1%20(Consumer%20Privacy%20-%20Version%203)_1.pdf
（2023 年 1 月 1 日施行）

CPRA は前述のように、CCPA を改正して成立したものであり、2023 年 1 月 1 日に施行されている。CPRA は、CPRA により新設されたカリフォルニア州プライバシー保護局（California Privacy Protection Agency、CPPA）及び州司法長官により執行される。CPRA に基づく民事上・行政上の執行は 2023 年 7 月 1 日から開始される[40]。なお、CPRA の施行規則であるカリフォルニア消費者プライバシー規則（California Consumer Privacy Regulations）[41]が 2023 年 3 月 29 日より施行されている。

イ　対象となる個人情報

[40] Cal. Civ. Code § 1798.185(d)
[41] https://cppa.ca.gov/regulations/pdf/20230329_final_regs_text.pdf

対象となる個人情報とは「特定の消費者又は世帯を識別し、関連し、記述し、合理的に関連付けることができ、又は直接的に若しくは間接的に合理的にリンクさせることのできる情報」をいう[42]。また、個人情報のなかでも、社会保障番号、運転免許証番号、州の身分証明書番号又はパスポート番号、高精度位置情報、人種若しくは民族的出自、宗教・思想上の信念又は組合員か否か、手紙・メール等の内容、遺伝情報、消費者を一意に識別するための生体認証情報、消費者の健康に関し収集及び分析された個人情報、消費者の性生活又は性的指向に関し収集及び分析された個人情報等は「機微個人情報（senstitive personal information）」として特別の保護の対象となっている[43]。

ウ　義務の対象者

CPRA の規制対象である「事業者」（Business）は、①カリフォルニア州で事業を行う者のうち、以下のいずれかを満たすもの (i)1 月 1 日の時点で、前年の年間売上高が 2500 万ドルを超えていること、(ii)独自に又は共同で、年間合計 10 万件以上の消費者又は世帯の個人情報を、購入、販売又は共有していること(iii)年間売上高の 50%以上を消費者の個人情報の販売又は共有から得ている者、 ② ①の事業者を支配し又は支配され、①の事業者と共通のブランドを有し、①の事業者が個人情報を共有する者 、③ ①の事業者がそれぞれ 40%以上の持ち分を有するジョイントベンチャー又はパートナーシップ、 ④ カリフォルニア州で事業を行う者のうち、上記①～③のいずれにも該当せず、CPPA に対し、CCPA を遵守し、CCPA に拘束されることを自発的に証明する者、である。

エ　義務及び禁止事項等

事業者の義務は多岐にわたるが、主要なものとしては、①利用目的等の通知義務（取得される個人情報の種類・利用目的・販売又は共有の有無、機微個人情報がある場合にはその種類・利用目的・販売又は共有の有無、機微個人情報の保持期間、その開示が不可能な場合は当該期間を定めるために利用される基準、プライバシーポリシーの公表義務 ）、②通知の態様（消費者に対する開示又はコミュニケーションは、消費者にとり読み易く理解し易いものでなければならない。例えば、平易かつ直接的な言葉を用い、かつ、専門用語又は法律用語を避けなければならないとする義務）③個人情報の取集、利用、保存及び共有を目的達成に必要かつ比例な程度とする最小化義務、④収集した個人情報を第三者に販売若しくは共有又はサービス提供者に開示する場合は、当該相手方と一定の規定のある契約を締結する義務、⑤保持期間の限定義務、⑥削除請求への対応義務 、⑦訂正請求への対応義務 、⑧オプトアウト手続の義務、⑨未成年者についてのオプトアウ

[42] Cal. Civ. Code § 1798.140(v)
[43] Cal. Civ. Code § 1798.140(ae)

ト義務、⑩機微個人情報についての制限義務、⑪安全管理義務等がある。なお、公的機関の命令等、人の死亡又は重症の危機の際の緊急アクセスの場合や、CMIA（以下に定義される。）に定める医療情報、HIPAA 及び経済的及び臨床的健全性のための医療情報技術に関する法律（Health Information Techonology for Ecnomic and Clinical Health Act、HITECH）によって定められた規制対象又は健康情報、CMIA に定めるヘルスケア提供者等については、CPRA の適用除外とされている。

(2) カリフォルニア州医療情報秘匿法(Confidentiality of Medical Information Act 、以下「CMIA」という。)

ア URL[2]

https://leginfo.legislature.ca.gov/faces/codes_displaySection.xhtml?sectionNum=56.10.&lawCode=CIV
（Cal. Stats. 1981, Ch. 782§1.5 により 1981 年成立）[44]

イ 対象となる個人情報

患者の名前、住所、メールアドレス、電話番号、社会保障番号など単独又は組み合わせにより個人の身元が明らかになる情報といった、医療提供者、医療サービス計画、製薬会社、又は委託業者（contractor）が保持し、そこから由来する、電子的又は物理的な形態による、患者の病歴、メンタルヘルス申請情報、精神的又は身体的状態に関する、個人を特定できるあらゆる情報である「医療情報」が対象となる[45]。

ウ 義務の対象者

認可若しくは認定されたクリニック、薬局、医療施設などの医療提供者若しくは医療グループ、独立開業協会、医薬品給付マネージャー、又は医療サービス組織であり、医療サービス計画又は医療の提供者ではない個人又は団体を指す委託業者等（以下、「医療提供者等」という。）[46]。

エ 義務及び禁止事項等

医療提供者等は、原則的に患者の医療情報を患者の承認を得ずに開示してはならず、医療提供者等及びその関連会社は、医療情報をマーケティングその他患者への医療の提供に必要のない目的で共有、販売又は使用してはならない[47]。また、医療

---

[44] Cal. Stats. 1981, Ch. 782 § 1.5 により、1979 年の同名法 Cal. Stats. 1979 Ch. 773 § 1 を廃止して成立した。
[45] Cal. Civ. Code §§56.05(i)
[46] Cal. Civ. Code §§56.05(d)(o)
[47] Cal. Civ. Code §§56.10(a)(d)

情報を作成、維持、保存、保管、放棄、破棄又はあ廃棄する医療提供者等は、そこに含まれる情報の機密性を保持する方法でそれらを行うものとする[48]。

(3) その他のカリフォルニア州法

遺伝子情報プライバシー法（Genetic Information Privacy Act, GIPA)は、①消費者主導型遺伝子検査製品（consumer-initiated genetic testing products）又はサービスを、直接消費者向けに提供する、②消費者から入手した遺伝子情報を分析する（医療技術の免許を受けた者による医療状態の診断又は治療のための分析を除く）又は③消費者に直接取引型遺伝子検査製品若しくはサービスから収集若しくは派生した、若しくは消費者から直接提供された遺伝子情報の収集、利用、保存又は開示する者を消費者直接取引遺伝子検査会社として[49]、その会社は遺伝子情報の収集、使用、保存及び開示に関する会社の方針及び手続について明確かつ完全な情報を提供し、遺伝子情報の収集、使用、維持及び開示について消費者の明示的な同意を得るものとしている[50]。また、会社は、消費者の同意の取消しのための仕組みを提供し、同意の取消しから 30 日以内に消費者の生体サンプルを破棄するものとされている[51]。但し、CMIA に準拠する医療情報、医療提供者について又は HIPAA に基づく事業提供者等は、適用除外とされている[52]。

その他、医療関係の情報についてのプライバシー規定としては、物理的安全管理措置（Physical Safeguards）として、医療提供者は患者の医療情報のプライバシー保護のため適切なセーフガードを確立し、実施し、不正なアクセス、使用・開示から医療情報を保護するものとされている[53]といった規定や、健康記録への患者のアクセス[54]、臨床検査の結果の患者への提供[55]などの個別法が存在する。

2 個人情報の保護に関する制度についての指標となり得る情報

(1) EU の十分性認定[36]

現時点において、カリフォルニア州を含む米国と EU 間では十分性認定はなされていない。[37]

(2) APEC の CBPR システム[38]

[48] Cal. Civ. Code §§56.101(a)
[49] Cal. Civ. Code § 56.18(b)(5)
[50] Cal. Civ. Code § 56.181(a)
[51] Cal. Civ. Code § 56.181(b)(c)
[52] Cal. Civ. Code § 56.184(c)(1)(2)(3)
[53] Cal. HS. Code § 1280.18(a)
[54] Cal. HS. Code § 123111
[55] Cal. HS. Code § 123148(a)

米国は 2012 年 7 月 25 日付で、APEC による CBPR システムへの参加を認められている[39]。

3　OECD プライバシーガイドライン 8 原則

OECD プライバシーガイドライン 8 原則の内、「①収集制限の原則」[56]、「②データ内容の原則」[57]、「③目的明確化の原則」[58]、「④利用制限の原則」[59]、「⑤安全保護の原則」[60]、「⑥公開の原則」[61]及び「⑦個人参加の原則」[62]については、CPRA に規定が存在する。なお、明文にないものの、「⑧責任の原則」としては、行政による制裁金というサンクションが予定されており[63]、データ管理者は、一定程度は、上記の諸原則を実施するための措置に従う責任を有しているということができる。

4　その他本人の権利利益に重大な影響を及ぼす可能性のある制度

(1) 個人情報の域内保存義務に係る制度であって、本人の権利利益に重大な影響を及ぼす可能性のあるもの

この点を明示する制度は見当たらない。

(2) 事業者に対し政府の情報収集活動への協力義務を課す制度であって、本人の権利利益に重大な影響を及ぼす可能性のあるもの

この点を明示する制度は見当たらない。

第3　イリノイ州法

1　個人情報の保護に関する制度の有無

イリノイ州では、現時点において、包括的なプライバシー規定は制定されていない[64]。しかし、規制対象となるデータの種類によっては、その取扱い等を個別に規制するイリノイ州法上の規定が存在する。イリノイ州法上の主なプライバシー規定は以下のとおりである。

(1) 個人情報保護法（Personal Information Protection Act、以下「PIPA」という。）

---

56 Cal. Civ. Code § 1798.100
57 Cal. Civ. Code § 1798.100(c)
58 Cal. Civ. Code § 1798.100(a)(1)(2)
59 Cal. Civ. Code § 1798.100(a)(1)(2)
60 Cal. Civ. Code § 1798.100(e)
61 Cal. Civ. Code § 1798.100(b)
62 Cal. Civ. Code § 1798.105,106,110
63 Cal. Civ. Code § 1798.155
64 One Trust DataGuidance, *Illinois*, (last visited Jun 12, 2023), https://www.dataguidance.com/jurisdiction/illinois

ア　URL[2]

https://www.ilga.gov/legislation/ilcs/ilcs3.asp?ActID=2702&ChapterID=67
（2006 年 1 月 1 日施行）

イ　対象となる個人情報

イリノイ州における個人情報保護法である PIPA[65]の下では、「個人情報（personal information）」の取り扱いに関する規制を設けており、PIPA における「個人情報」とは、（１）個人の名前、若しくは名前のイニシャルと苗字を合わせたものを、同人の社会保障番号、運転免許証番号、医療や保健情報等と紐づけたもの、又は（２）ユーザー名若しくはメールアドレスを、パスワード若しくは本人認証のための質問（及び当該質問への答え）と紐づけたものを指す[66]。但し、上記（１）及び（２）において、該当情報が暗号化（encrypted）若しくは削除（redacted）されている場合は、非暗号化も氏 h くは削除された情報の復元か可能でない限り、個人情報とはみなされないとされる[67]。また、PIPA 下の個人情報には、連邦・州・地方自治体政府により公開されている情報は含まれない[68]。上記の個人情報の内、「医療情報（medical information）」は個人の医療履歴、身体・精神状態に関する情報、医療従事者による治療・診断情報を指し[69]、「保険情報（health insurance information）」は個人の保険番号や保険会社により使用される識別子、また個人の保険申請書に含まれる医療情報等を指す[70]。

ウ　義務の対象者

PIPA の対象となる「データ収集者（data collector）」は、その目的を問わず、非公開の個人情報の処理、収集、拡散又はその他取り扱いを行うものとされ、その一例として、政府機関、大学、企業、金融機関、小売業者等が挙げられている[71]。

エ　義務及び禁止事項等

PIPA の対象となるデータ収集者は、自身が所持するイリノイ州民に関する個人情報の漏洩等があった場合、原則として関連する個人へ速やかに所定の通知を行う必要がある[72]。通知の方法としては、書面通知、電子通知、又は代替通知[73]が認め

---

[65] 815 ILCS 530/1
[66] 815 ILCS 530/5
[67] 815 ILCS 530/5
[68] 815 ILCS 530/5
[69] 815 ILCS 530/5
[70] 815 ILCS 530/5
[71] 815 ILCS 530/5
[72] 815 ILCS 530/10(a)
[73] 815 ILCS 530/10(c)。なお、代替通知（substitute notice）とは、通知を行うための費用が$250,000 を超える、被害者の数が 500,000 人を超える、もしくはデータ収集者が要求される通知に必要な情報を持っていない場合にお

られている。また、データ漏洩等で影響を受けたイリノイ州民の数が 500 人以上である場合は、別途イリノイ州司法長官への通知が求められる[74]。加えて、イリノイ州民の個人情報を含む記録を有するデータ収集者は、当該記録に関する合理的な保護措置を設けなければならない[75]。

(2) イリノイ州生生体情報プライバシー保護法（Illinois Biometric Information Privacy Act、以下「BIPA」という。）

ア URL[2]

https://www.ilga.gov/legislation/ilcs/ilcs3.asp?ActID=3004&ChapterID=57
（2008 年 10 月 3 日施行）

イ 対象となる個人情報

BIPA の下では、「生体情報（biometric information）」及び「生体識別子（biometric identifier）」等の取り扱いに関する規制がなされている。この内、「生体情報」については「その取得、変換、保存、共有の方法を問わず、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情報」[76]と定義され、「生体識別子」は「網膜や虹彩のスキャン、指紋、声紋、又は手や顔の形状のスキャン」[77]と定義されている。一方で、生体識別子の定義からは様々な情報が除外されており、例えば、筆記サンプル、署名、写真、科学的試験やスクリーニングのために使用される生体サンプル、身長、体重、目や髪の色、X 線、MRI 若しくは PET スキャンの画像等は含まれないとされている[78]。

ウ 義務の対象者

BIPA の下では、主に生体情報又は生体識別子を扱う「民間対象者（private entity）」に対する規制を設けている。「民間対象者」は、「個人、パートナーシップ、会社、有限責任会社、協会又はその他の団体であり、その組織形態を問わない」[79]と広範囲に定義されている。

エ 義務及び禁止事項等

いて、メールでの通知（メールアドレスがある場合）、自身のウェブサイト上での告知、及び州メディア（場合によっては地方メディアも可）媒体を通じた告知の全てを行うことにより、PIPA 上の通知要件を満たすことを指す。

[74] 815 ILCS 530/10(e)(2)
[75] 815 ILCS 530/45
[76] 740 ILCS 14/10
[77] 740 ILCS 14/10
[78] 740 ILCS 14/10
[79] 740 ILCS 14/10

BIPA の規制を受ける民間対象者は、自身が所持する生体情報及び生体識別子の保持に関するスケジュールやそれらの破棄に関するガイドライン等を明記したポリシーの作成及び公開をしなければならない[80]。また、禁止事項として、当該民間対象者は原則的に、関連する個人への事前通知並びに本人からの事前承諾無しに、本人の生体情報及び生体識別子の収集[81]や開示[82]等を行ってはならないとされている。加えて、生体情報及び生体識別子の販売、賃貸、交換その他利益が生じる行為[83]も禁止されている。民間対象者が所持する生体情報及び生体識別子は、合理的な標準の保護措置の下保管されなければならない[84]。

(3) 遺伝情報プライバシー保護法（Genetic Information Privacy Act, 以下「GIPA」という。）

ア URL[2]

https://www.ilga.gov/legislation/ilcs/ilcs3.asp?ActID=3004&ChapterID=57
（1998 年 1 月 1 日）

イ 対象となる個人情報

GIPA の対象となる「遺伝情報（genetic information）」[85]は、医療保険の携行性と責任に関する法律（Health Insurance Portability and Accountability Act of 1996: HIPAA）同定義と紐づけされており、個人又はその家族の遺伝子テストに関する情報のみならず、個人の家族に生じた病気や障害に関する情報等も含まれている。但し、個人の性別及び年齢に関する情報は含まれない[86]。

ウ 義務の対象者

GIPA における「対象者（covered entity）」[87]の定義は、HIPAA における同定義と紐づけされており、主に、HIPAA の規制を受ける活動に関連して医療情報を電子的に送信する医療サービス提供者が対象となっている[88]。

エ 義務及び禁止事項等

---

[80] 740 ILCS 14/15(a)
[81] 740 ILCS 14/15(b)
[82] 740 ILCS 14/15(d)。なお、BIPA における生体情報及び生体識別子の開示に関しては、連邦・州・地方自治体による法令や、裁判所の命令によって開示が求められる場合は例外的に開示が認められるものとされる。
[83] 740 ILCS 14/15(c)
[84] 740 ILCS 14/15(e)
[85] 410ILCS 513/10
[86] 45 CFR 160.103
[87] 410ILCS 513/10
[88] 45 CFR 160.103。なお、当該「対象者（covered entity）」の定義には、この他に、健康保険及び医療情報センターが含まれる。

GIPA 冒頭では、まず、遺伝情報を機密情報と位置づけ、原則として当人又は同人が書面によって承認した者以外には開示されてはならないとしている[89]。但し、一定の場合においては対象者による個人の承諾無しでの遺伝情報の開示が認められており、例えば、対象者による治療や支払工程のためや[90]、医療サービス提供者による治療のために開示される場合[91]等は事前に承諾を得る必要が無いとされる。その他、対象者はその業務関係者（business associate）に対し、自身に代わって HIPAA の対象となる医療情報（protected health information）の作成、受領、保管、送信を行わせる場合に、当該業務関係者が適切に当該情報を保護できるという保証を得れば、個人の承諾無しで遺伝情報の開示を行う事ができるとされている[92]。また、GIPA では雇用者による従業員への遺伝子テストの強要や、遺伝子テストの有無や遺伝情報等に基づく不当な従業員の扱い等を禁じている[93]。

（4）その他のイリノイ州法

上記の法令の他にも、イリノイ州法には異なる健康情報の扱いを規制する法令がいくつか見られる。例えば、医療患者権利法（Medical Patient Rights Act）[94]では、内科医、医療サービス提供者、保険会社等による、患者の健康情報の開示を制限している。病院ライセンシング法（Hospital Licensing Act）[95]においては、病院に対し、患者の記録の機密性の尊重等を義務付けている。また、2022 年 1 月 1 日に施行開始した家庭プライバシー保護法（Protecting Household Privacy Act: PHPA）[96]では、イリノイ州の法執行機関による各家庭の電子データ（household electronic data）の収集等に関する規制を設けている。この他、イリノイ州法では、歯科医療情報[97]、薬物乱用に関する情報[98]、メンタルヘルスに関する情報[99]、AIDS[100]その他性感染症[101]に関する情報等をそれぞれ個別の法令で規制している。

2　個人情報の保護に関する制度についての指標となり得る情報

（1）EU による十分性の認定[36]

現時点において、イリノイ州を含む米国と EU 間では十分性認定はなされていない[37]。

---

89 410 ILCS 513/15(a)
90 410 ILCS 513/31(1)
91 410 ILCS 513/31(2)
92 410 ILCS 513/31.3(a)
93 410 ILCS 513/25
94 410 ILCS 50/0.01
95 210 ILCS 85/1
96 5 ILCS 855/1
97 215 ILCS 109/1
98 20 ILCS 301/1-1
99 740 ILCS 110/1
100 410 ILCS 305/1
101 410 ILCS 325/1

(2) APEC による CBPR システムへの参加[38]

米国は 2012 年 7 月 25 日付で、APEC による CBPR システムへの参加を認められている[39]。

3 OECD プライバシーガイドライン８原則

OECD プライバシーガイドライン 8 原則の内、「①収集制限の原則」[102]、「③目的明確化の原則」[103]、「④利用制限の原則」[104]、「⑤安全保護の原則」[105]、「⑥公開の原則」[106]及び「⑦個人参加の原則」[107]については、BIBA に部分的な関連項目が見受けられる。また、「⑤安全保護の原則」については、PIPA[108]にも一部対応すると思われる項目が見られる。

4 その他本人の権利利益に重大な影響を及ぼす可能性のある制度

(1) 個人情報の域内保存義務に係る制度であって、本人の権利利益に重大な影響を及ぼす可能性のあるもの

この点を明示する制度は見当たらない。

(2) 事業者に対し政府の情報収集活動への協力義務を課す制度であって、本人の権利利益に重大な影響を及ぼす可能性のあるもの

この点を明示する制度は見当たらない。

第4 ニューヨーク州法

1 個人情報の保護に関する制度の有無

ニューヨーク州憲法やコモン・ローは、プライバシー権について明示的に規定していない。また、現時点でニューヨーク州は、個人情報保護につき包括的（分野横断的）な法令を置いていない。しかし、規制対象となるデータの種類によっては、その取扱い等を個別に規制するニューヨーク州法上の規定が存在する。

(1) ニューヨーク州公民権法（Civil Rights Law、以下「NYCRL」という。）

ア URL[2]

https://law.justia.com/codes/new-york/2022/cvr/article-7/79-l/
（2017 年 3 月 1 日施行）

---

102 740 ILCS 14/15(b)
103 740 ILCS 14/15(b)(2)
104 740 ILCS 14/15(b)-(d)
105 740 ILCS 14/15(e)
106 740 ILCS 14/15(a)
107 740 ILCS 14/15(b)(3)
108 815 ILCS 530/45, 前掲注 21

イ　対象となる個人情報

NYCRL 7 条 9 号 L は、「遺伝子検査記録の秘密（Confidentiality of Records of Genetic Tests）」に関して規定を設けている[109]。本法がいう「生体試料（biological sample）」とは、人体の一部若しくは排出物であって、DNA を含むもの（組織、血液、又は尿を含むがそれに限定されない）である。

ウ　義務の対象者

NYCRL は、ニューヨーク州管轄内の全ての個人に適用される。

エ　義務及び禁止事項等

NYCRL によれば、何人も、別段の定めがある場合を除き、当該本人の書面による事前の同意がなしに、生体試料に対し遺伝子検査を実施してはならない（本法にはこの同意の際に書面上含めておくべき事項についても詳細な規定がある）。また、本法によれば、いかなる人に対しても、実施された遺伝子検査記録、所見及び結果は秘密とされ、当該遺伝子検査が関係する人物の同意がない限り開示されない。これらの禁止事項に違反した者には、1000 ドル以下の民事制裁金が課されるほか、故意に違反した者には、5000 ドル以下の罰金、90 日以下の拘禁、又はその両方が課される。

但し、本法は、研究又は統計目的のために、審査委員会が承認した研究手順に基づき、提供者の匿名性が担保された試料を用いて遺伝子検査を実施したり、同意対象遺体の検査に利用したりすることもできる、という例外規定を置いている。

(2) ハッキング禁止及び電子データセキュリティ改善に関する法律（New York Stop Hacks and Improve Electronic Data Security Act）（以下「SHIELD 法」という。）

ア　URL[2]

https://www.nysenate.gov/legislation/bills/2019/s5575
（2020 年 3 月 21 日施行）

イ　対象となる個人情報

SHIELD 法の「個人情報（personal information）」とは、自然人に関する情報であって、氏名、番号、個人的な特徴又はその他の識別子により、当該個人を特定可能なもの、をいう。また、本法の「私的情報（private information）」とは、①(1)社会保障番号、(2)運転免許証番号又は非運転者特定証番号、(3)口座番号、クレジット・デビットカード番号、及びそのセキュリティコード、アクセスコード、パ

[109] NY Civ Rights L § 79-L (2022).

スワードその他個人の金融口座へのアクセスを許可する他の情報、⑷（セキュリティコード、アクセスコード又はパスワードその他識別情報なしに個人の口座へのアクセスが可能な場合の）口座番号、クレジット・デビットカード番号、⑸生体認証情報、のいずれか１つと個人情報の組み合わせに加えて、②ユーザー名又はメールアドレスと、オンラインアカウントへのアクセスを可能とする秘密の質問及びその答えとの組み合わせ、をいう。

ウ　義務の対象者

本法は、私的情報を含む電子化された情報を所有、ライセンス又は管理している自然人又は事業者に適用される。

エ　義務及び禁止事項等

私的情報を含む電子化された情報を所有、ライセンス若しくは管理している自然人又は事業者は、保有若しくは使用を許諾している私的情報を含む電子化された情報の不正な取得やアクセスを発見し又はその通知を受けた場合には、その不正取得等の対象となる私的情報が帰属するニューヨーク州居住者へその事実を通知しなければならない。また、そのような自然人又は事業者は、手続的、技術的、物理的措置を含む情報セキュリティ措置も実施しなければならない。

この通知義務、セキュリティ措置義務の違反それぞれ、罰金等の制裁が用意されている。

⑶ 個人プライバシー保護法（Personal Privacy Protection Law，以下「PPPL」という。）

ア　URL[2]

https://opengovernment.ny.gov/personal-privacy-protection-law
（1984 年施行）

イ　対象となる個人情報

「個人情報（Personal Information）」、すなわち氏名、記号、標章その他の識別情報により個人を識別できる情報の取扱いに関する規定を設けている[110]

ウ　義務の対象者

[110] NY Pub Off L § 92 (2012).

「公的な機関（Agency）」であり、州の委員会、審議会、部局その他の政府機関又は同様の役割を果たす機関である。但し、司法権、州議会や地方自治体は除く。

エ　義務及び禁止事項等

PPPL によれば、政府が「個人情報」を収集できるのは法目的達成に「関連し、必要である（relevant and necessary）」場合のみであり[111]、収集にあたってはその理由、保管場所、利用方法を説明しなければならない[112]。また、「個人情報」が保管された場合には、同意なく開示されず（法律の規定がある場合を除く）[113]、アクセス権や訂正権も認められる[114]。

(4) その他のニューヨーク州法[115]

金融サービス局サイバーセキュリティ規則（New York Cybersecurity Requirements for Financial Services Companies）においては、銀行法、保険法、若しくは金融サービス法に基づきライセンス等を受けて業務を行う、又は行うべき全ての事業体に対し、「非公開情報（nonpublic information）」[116]について、情報システムの機密性等が確保されるよう設計されたサイバーセキュリティプログラムを維持しなければならず、加えて取締役会等により承認されたセキュリティポリシーを定めなければならないとされている。

このほか、公衆衛生法（Public Health Law）には、性感染症[117]、先天性異常及び遺伝的疾患[118]、HIV[119]といった情報の取扱いについて、精神衛生法（Mental Hygiene Law）

---

111 NY Pub Off L § 94 (2012).
112 *Id*.
113 NY Pub Off L § 96 (2012).
114 NY Pub Off L § 94 (2012)
115 現在、生体認証プライバシー法（Biometric Privacy Act）案 が提出され、上院の消費者保護委員会に係属している。同法案は、民間団体が生体認証識別子や生体認証情報を取得する際の手続を定めるとともに、民間団体に対し、収集目的を達成すれば当該情報を完全に廃棄するための規則を書面で定めておくよう義務付けるものである 。また、NY プライバシー法（NY Privacy Act）案 も提出され、上院の消費者保護委員会を通過した。同法案は、2018 年にカリフォルニア州で制定された消費者プライバシー法（California Consumer Privacy Act: CCPA）と同様の、包括的なプライバシー法である。
116 「非公開情報（nonpublic information）」を対象としている。この「非公開情報」とは、一般に公開されていない電子情報であって、①対象事業者の事業関連情報で、改ざんまたは不正な開示、アクセスもしくは利用により、対象事業者の事業、運営またはセキュリティに重大な悪影響を及ぼし得るもの、②⑴社会保障番号、⑵運転免許証番号または非運転者特定証番号、⑶口座番号、クレジットカード・デビットカード番号、⑷口座にアクセスするためのセキュリティコード、アクセスコード、またはパスワード、⑸生体認証情報のいずれか 1 つの組み合わせにより、個人を識別できる情報、または③医療提供者もしくは個人により作成または個人から得られた、⑴個人またはその家族の過去現在将来の身体、精神、行動的な健康状態、⑵個人への医療提供状況、⑶個人への医療提供に対する支払い状況に関連する情報（ただし年齢・性別を除く）をいう。
117 NY Pub Health L § 2306 (2022)
118 NY Pub Health L § 2733 (2022).
119 NY Pub Health L § 2782 (2022).

には、アルコール依存症や薬物乱用[120]の情報の取扱いについて個別の定めが置かれている。

2　個人情報の保護に関する制度についての指標となり得る情報

(1) EU の十分性認定[36]

現時点において、ニューヨーク州を含む米国と EU 間では十分性認定はなされていない[37]。

(2) APEC の CBPR システム[38]

ニューヨーク州を含む米国は 2012 年 7 月 25 日付で、APEC による CBPR システムへの参加を認められている[39]。

3　OECD プライバシーガイドライン８原則

OECD プライバシーガイドライン 8 原則のうち、「①収集制限の原則」、「②データ内容の原則」、「③目的明確化の原則」、「④利用制限の原則」、「⑤安全保障の原則」「⑧責任の原則」について、上述した法令の規定が対応する。

4　その他本人の権利利益に重大な影響を及ぼす可能性のある制度

(1) 個人情報の域内保存義務に係る制度であって、本人の権利利益に重大な影響を及ぼす可能性のあるもの

この点を明示する制度は見当たらない。

(2) 事業者に対し政府の情報収集活動への協力義務を課す制度であって、本人の権利利益に重大な影響を及ぼす可能性のあるもの

この点を明示する制度は見当たらない。

第5　留意すべき事項

- 個人情報の保護に関する法律（平成 15 年法律第 57 号）（以下「個人情報保護法」という。）第 28 条第 2 項の趣旨には、外国にある第三者に対する個人データの提供に伴うリスクについて、本人の予測可能性を高めるという点のほか、外国にある第三者に対して個人データを提供する事業者においても、提供先の外国にある第三者における事業環境等を認識することを促すという点が含まれる。また、事業者が同項に基づいて本人に対して提供すべき情報の具体的内容は、個別の事案に応じて異なり得る。外国における個人情報の保護に関する制度の確認は、外国にある第三

[120] NY Ment Hygiene L § 22.05 (2022).

者に対して個人データを提供する事業者の責任が個別具体の状況を踏まえてさらに調査を実施し、説明することは有益であり推奨されるものである。

- 上記情報は、あくまで調査を実施した 2023 年 6 月の時点における情報に基づくものである。当該時点以降、外国において個人情報の保護に関する制度が改正されること等により、外国にある第三者に対して個人データを提供する事業者が本人に対して提供すべき情報の内容にも変更が生じる可能性がある。
- 上記情報は、以下の観点から調査対象の法令を限定して行ったものであり、必ずしも網羅的なものではない。外国にある第三者に対して個人データを提供する事業者は、上記情報以外にも関連する情報を保有している場合には、個人情報保護法第 28 条第 2 項及び個人情報の保護に関する法律施行規則（平成 28 年個人情報保護委員会規則第 3 号）第 17 条第 2 項に基づき、当該情報も本人に対して提供する必要がある。