



基
般

アメリカのプライバシー保護に関する動向

石井 夏生利 筑波大学図書館情報メディア系

最近のプライバシー保護をめぐるアメリカの状況

本稿では、アメリカのプライバシー保護をめぐる最近の動きを取り上げる。

アメリカのプライバシー保護法制は、公的部門に関しては、1974年プライバシー法（Privacy Act of 1974）が制定され、民間部門に関しては、自主規制を基本とし、機密性が高い情報を扱う分野において、数多くの個別法が制定されてきた。規制対象を限定して個別領域ごとに立法措置を講じる方式は、セクトラル方式と呼ばれる。

このように、アメリカのプライバシー保護は、特に民間部門では緩やかといえる。他方、アメリカは、GoogleやFacebook、Twitter、Appleなどの巨大インターネット関連事業者を抱えており、ビッグデータを用いたビジネスを大規模に展開している。そのような中、ホワイトハウスが2012年2月に消費者データプライバシーに関する政策大綱、2014年5月にビッグデータに関する報告書を発表するなど、民間部門の個人情報の取扱いを規律することに向けた議論も行われている。また、民間部門では、連邦取引委員会（Federal Trade Commission：FTC）がプライバシーポリシーやセーフハーバー^{☆1}に違反した事業者に対して「不公正若しくは欺瞞的行為

^{☆1} 「セーフハーバー」とは、企業の行動が違法や違反とされない範囲を示したルールをいう。当局が企業活動に包括的規制を敷く際に、適法な範囲が明確でなければ、企業は予見可能性を得られないため、安全策をとって活動自体を避けるようになる。そうした事態を避けるため、セーフハーバーを設けて適法性の範囲を明確にする慣行が米国を中心に取り入れられている。

又は慣行」（FTC法第5条）に基づく法執行を行うとともに、消費者プライバシーに関する数多くの報告書を公表してきた^{☆2}。

州法レベルでもさまざまなプライバシー保護法が制定されているが、特に先進的な法律を成立させてきたのはカリフォルニア州である。同州が最初に制定したセキュリティ侵害通知（データ侵害通知）法については、ほぼすべての州が同様の法律を成立させたほか、アメリカ国外でも、EU（European Union）で審議が進められている一般データ保護規則提案の中に関連規定が設けられている。日本では、2014年7月にベネッセコーポレーションからの個人情報大量流出事件が大きく報じられ、個人情報保護法の改正事項にいわゆる名簿屋規制を導入する方向性となっているが、セキュリティ侵害通知法は、情報漏えいが発生した場合に事後的な通知や報告を義務づけるものである。アメリカでは、FTCがデータブローカに関する報告書を発表し、議会でもデータブローカ規制法案が提出されるなどの動きもある。

カリフォルニア州のプライバシー保護法

■ セキュリティ侵害通知法

カリフォルニア州はプライバシー保護に向けた積極的な取り組みを行う州である。その代表はセキュ

^{☆2} FTC法第5条に基づく法執行は、同意命令（一種の和解手続）で処理されることが多い。2011年から2012年にかけて、Googleが20年間の監査に服することや約2,000万ドルの制裁金を支払うことで合意した事例などがある。

リティ侵害通知法であり、同法は、2002年9月26日、州の民事法典（California Civil Code）を改正することにより成立した。同法は、州の機関および州の事業者に対し、州住民の暗号化されていない個人情報が無権限者によって取得され、または、取得されたと信じる合理的な理由があるときには、不当に遅延しない限りでの適切かつ可能な時期に、システムのセキュリティ侵害が生じた事実を本人に通知しなければならない義務を定めている。機関および州の事業者が、一度のセキュリティシステムの侵害の結果として、500名を超える州住民への通知を義務づけられる場合は、司法長官に対し、個人識別情報を除いた形で、セキュリティ侵害通知に関する1つの見本の写しを電子的に提出しなければならない。

2013年9月27日には、同法の改正法が成立した。改正法は、オンラインアカウント情報が侵害された場合におけるセキュリティ侵害通知の義務を拡大することを内容とする。

セキュリティ侵害通知法の定める「個人情報」は、改正前は、①個人の名前（first name）または先頭の頭文字および苗字（last name）を、社会保障番号（SSN）等の所定のデータ要素^{☆3}の1つ以上と組み合わせたものであって、氏名またはデータ要素のいずれかが暗号化されていないものをいうと定めていたが、それに加えて、②ユーザネームまたは電子メールアドレスであって、パスワードまたは安全のための質問および回答を組み合わせて、オンラインアカウントへのアクセスを可能にするものが追加された。

また、同法によると、個人情報を含むシステムのセキュリティ侵害が、②のオンラインアカウントのためのユーザネームまたは電子メールアドレスに関する場合であって、①の個人情報を含まないとき、州の機関は、セキュリティ侵害通知を電子的形式等で被害者に伝え、パスワードや、安全のための質問

または回答を迅速に変更させ、またはオンラインアカウントを保護するための他の措置を講じることができる。ただし、個人情報を含むシステムのセキュリティ侵害であって、オンラインアカウントへのアクセスを可能にするものが、州の機関の提供した電子メールアカウントのログイン認証に関するものである場合、かかる機関は、セキュリティ侵害通知をその電子メールアドレスに送ってはならず、文書による通知や、電子記録および電子署名に関する規定に準拠した電子的通知、他の明示的で分かりやすいオンライン上の通知等、他の手段によらなければならない。州の事業者に関しても、同内容の改正が行われた。

2014年4月11日現在、アラバマ州、ケンタッキー州、ニューメキシコ州およびサウスダコダ州を除いた46の州、コロンビア特別区、グアム、プエルトリコ、バージン諸島がセキュリティ侵害に関する法律を制定させている。

■ 消しゴム法

EUの一般データ保護規則提案では「忘れられる権利」が提案され、日本でも話題となった。インターネット上の情報を削除する権利との関係では、カリフォルニア州でも消しゴム法が制定され、忘れられる権利と比較して取り上げられることがある。同法は2013年9月23日に成立し、施行は2015年1月1日を予定している。同法によると、インターネット・Webサイト、オンライン・サービス、オンライン・アプリケーション、または、モバイル・アプリケーションの運営者であって、児童（州内に居住する18歳未満の自然人）向けのもを提供する者は、児童がそれらのサービスを利用しているという現実の認識を有している場合に、①利用者登録をした児童が当該サービスやサイト等に投稿したコンテンツを削除できるようにするとともに、②削除できる旨を児童に伝えること、③削除方法を明確に児童に説明すること、④当該削除が完全または全体的なコンテンツの削除を保証するものではない旨を児童に伝えることを義務づけられる。ただし、児童が

^{☆3} SSN、運転免許証番号またはカリフォルニア州のIDカード番号、口座番号またはクレジットもしくはデビットカード番号であって、求められるセキュリティコード、アクセスコードまたはパスワードとの組合せによって、個人の金融口座へのアクセスを可能にするもの、医療情報、健康保険情報。

投稿した情報を第三者が保存、再公開または再投稿した場合を含め、当該児童以外の第三者が保存または投稿したコンテンツである場合や、児童の投稿したコンテンツを運営者が匿名化し、児童を個人識別できないようにした場合等には、運営者または第三者は削除を義務づけられない。

■ Do Not Track

カリフォルニア州では、2013年9月27日、セキュリティ侵害通知に関する法律改正と同時に、追跡拒否 (Do Not Track : DNT) に関する法を制定させた。同法では、商用Webサイトまたはオンライン・サービスの運営者は、州内に居住し、商用Webサイトまたはオンライン・サービスを利用したまたは訪問する個人消費者に関して、その個人識別情報をインターネットを通じて収集する場合、Webサイト上に、目立つ形でプライバシーポリシーを載せる義務を負う。そのポリシーの中に、DNTの方法を含めることが義務づけられている。運営者は、時間をかけて、かつ、第三者のWebサイトやオンライン・サービスを介して、個人消費者のオンライン上の活動に関する個人識別情報を収集する場合、消費者に対し、その収集に関する選択を行使する能力を与える方法を開示しなければならない。

消費者プライバシー保護に向けた議論

■ 消費者データプライバシー

アメリカの消費者プライバシー保護の取り組みの中で、最近注目を集めたものの1つに、「消費者プライバシー権利章典」がある。2012年2月23日、Obama大統領は、「ネットワーク社会における消費者データプライバシー：グローバル化したデジタル経済において、プライバシーを保護しイノベーションを促進するための枠組み」(以下「消費者データプライバシー」という)に署名した。この政策大綱は、「消費者プライバシー権利章典」(表-1)、法的に執行可能な実施基準、FTC法第5条に関するFTCの法執行権限、国際的相互運用可能性を主な

第1原則 個人の コントロール	消費者は、企業が消費者からいかなる個人データを収集し、どのように利用するかについて、コントロールを行使する権利を有する。
第2原則 透明性	消費者は、プライバシーおよびセキュリティの実務について、容易に理解できアクセス可能な情報を得る権利を有する。
第3原則 状況の尊重	消費者は、企業において個人データを収集し、利用し、そして提供する際には、消費者がデータを提供する状況に適合した方法によることを期待する権利を有する。
第4原則 安全性	消費者は、安全かつ責任を持って個人データが取り扱われる権利を有する。
第5原則 アクセスおよび 正確性	消費者は、データの機微性およびデータが不正確な場合に消費者に不利な結果をもたらすリスクに適した態様において、利用可能な書式によって、個人データにアクセスし、訂正する権利を有する。
第6原則 制限的収集	消費者は、個人データを収集および保有する企業に適切な制限を課す権利を有する。
第7原則 責任	消費者は、企業が個人データを取り扱う際に、消費者プライバシー権利章典を確実に厳守するための適切な措置とともにに行わせる権利を有する。

表-1 消費者プライバシー権利章典

要素に掲げている。

消費者プライバシー権利章典は、アメリカが1970年代からプライバシー保護立法の中に取り入れてきた公正情報実務諸原則 (Fair Information Practice Principles : FIPPs) を基礎とする諸原則である。

消費者データプライバシーは、消費者プライバシー権利章典の実施方法として、執行可能な実施基準を展開するためのマルチステークホルダプロセス、FTCに執行権限を付与することを伴う権利章典の連邦法による立法化に言及している。

■ FTC プライバシー・レポート

FTCは、1990年代後半頃より、消費者プライバシー保護への取り組みを積極的に行うようになり、2007年頃からは、行動ターゲティング広告との関係で、重要な報告書を公表している。その1つとして、2012年3月26日、事業者および政策立案者向けの枠組みとしての「急変する時代の消費者プライバシー保護」(以下「FTC プライバシー・レポート」という)が発表された。このレポートでは、プライバシー・バイ・デザイン (Privacy by Design :

PbD), 単純化した消費者の選択, 透明性の3つが
 枠組み勧告として示された。PbDとは、製品およ
 びサービスのライフサイクル全体にわたって、プ
 ライバシー保護を組み込むという考え方であり、カナ
 ダのオンタリオ州がその発祥である。EUの一般デ
 ータ保護規則提案の中にも PbD の定めが置かれて
 いる。

また、FTCは、今後1年の間に取り組む主要事
 項として、①DNTの仕組みの推進、②携帯電話サ
 ービス提供事業者によるプライバシー保護の改善、
 ③データブローカによる消費者情報の収集利用をコ
 ントロールするための立法化提案、④ISP (Internet
 Service Provider) や OS (Operating System) 提
 供者等の大規模プラットフォーム事業者による消費
 者行動の追跡への対応、⑤FTC法第5条に基づく
 執行可能な自主規制基準の推進の5つを挙げている。
 この方向性は現時点でも変わっていない。

■ ビッグデータに関する報告書

2014年5月1日、大統領行政府から「ビッグデ
 ータ：機会を捉え価値を維持する」と題する報告書
 が公表された。これは、ビッグデータが社会関係に
 与える変化等に基づき、Obama大統領から政府の
 政策方針を検討するよう指示を受け、大統領補佐官
 (Counselor to the President) であるジョン・ポデ
 スタ (John Podesta) 氏を含む5名の高官の連名に
 おいて、大統領に提出したものである。報告書は、「第
 1章 ビッグデータと個人」、「第2章 オープン・
 データとプライバシーに向けたObama政権のアプ
 ローチ」、「第3章 公的部門のデータ管理」、「第4
 章 民間部門のデータ管理」、「第5章 ビッグデー
 タの政策枠組に向けて」、「第6章 結論及び勧告」
 で構成される。報告書は、全体的に消費者データプ
 ライバシーよりも広い範囲の問題を取り扱っている。
 第6章では、消費者プライバシー権利章典の立法化
 を含め、6項目の政策提言が示された(表-2)。第
 2項目の国のデータ侵害法の制定は、連邦レベルで
 のセキュリティ侵害通知法を定めようとする提言で
 ある。

消費者プライバ シー権利章典の 促進	商務省は、ビッグデータの展開およびそれが どのように消費者プライバシー権利章典に影響を 与えるかについて、ステークホルダーおよ び一般からの意見を求めるための適切な協 議段階に入るべきである。そして、ステーク ホルダーが検討を行い、大統領から議会へ提 出するための立法草案を案出すべきである。
国のデータ侵害 法の制定	議会は、2011年5月の政府によるサイバー セキュリティ立法提案に従って、単一の国家 データ侵害基準を定める立法を可決すべきで ある。
米国人以外への プライバシー保 護の拡大	行政予算管理局は、実行可能な場合には1974 年プライバシー法を米国人以外にも適用する か、または、国籍にかかわらず、適切かつ意 味ある保護を個人情報に適用する代替的プ ライバシー政策を確立するよう、各省庁および 機関と協力すべきである。
学校において収 集される生徒の データを確実に 教育目的で利用 すること	連邦政府は、プライバシー規制により、特に 教育の状況において集められたデータが不適 切に共有されたり利用されたりすることから 生徒を確実に保護しなければならない。
差別を阻止する ための技術専門 性の拡大	公民権や消費者保護を主導する連邦政府の各 機関は、ビッグデータ分析により促進される 実務および結果であって、保護される階級へ の差別的影響を有するものを特定できるよう に、また、違法行為の捜査や解決のための計 画を立てられるように、技術専門性を拡大す べきである。
電子通信プライバ シー法の改正	議会は、オンライン、デジタルコンテンツの ための保護水準が実社会において与えられる もの—未読の電子メールや一定期間を経過し たもの—のような、時代遅れの区別を撤廃す ることを含むと確実に合致するよう、電子通 信プライバシー法を改正すべきである。

表-2 ビッグデータに関する報告書の政策提言

データブローカと透明性

■ データブローカに関する報告書

日本の個人情報保護法改正については、ベネッセ
 コーポレーションからの情報漏えい事件を受け、名
 簿屋規制が検討されているが、アメリカで名簿屋
 に相当する事業者は「データブローカ」(data bro-
 kers)といわれている。データブローカは、個人に
 関する情報をあらゆるソースから収集・分析してカ
 テゴライズを行い、第三者へ販売することを主な事
 業分野にする企業のことをいい、アメリカでは、ア
 クシオム (Acxiom) を始めとする有名事業者が複
 数存在する。

データブローカの問題は、前記の消費者データプ
 ライバシー、ビッグデータに関する報告書、FTC

のプライバシー・レポートのほか、政府監査院 (Government Accountability Office : GAO) が 2013 年 9 月に上院の通商科学運輸委員会の議長であるジョン・D・ロックフェラー 4 世 (John D. Rockefeller IV) あてに提出した「情報再販者：消費者プライバシーの枠組みに、技術および市場の変化を反映させる必要あり」と題する報告書でも取り上げられている。いずれの文書も、データブローカが消費者との直接の関係を持たず、消費者がデータブローカの実務を認識・理解していないこと、現行法上の規制が存在しないことを指摘している。GAO の報告書は、包括的な連邦プライバシー法が存在しないという問題を述べ、FTC のプライバシー・レポートは、透明性向上を主張している。

FTC は、データブローカに焦点を当てた報告書として、2014 年 5 月 19 日、「データブローカ 透明性及び説明責任の要請」を公表した。報告書では、規制面の観点から、データブローカのサービス類型として、公正信用報告法^{☆4}に基づく消費者報告機能、潜在顧客を明らかにするマーケティング、本人確認や欺罔行為探知等のリスク緩和、公開情報から消費者を探知する「人探し」サイト^{☆5}が示されている。そして、かかるデータブローカに関する FTC の認識事項は、次のように、事業の性質、便益およびリスク、消費者の選択という 3 項目に整理されている (表-3)。

■ FTC の立法化提言

報告書は、これらの認識事項により、データブローカ産業の実務についての透明性が基本的に欠如していると指摘した。そして、全会一致の委員会の勧告事項として、議会に対し、①マーケティング商品、②リスク緩和商品、③人探しに分けて、次のような立法化を検討するよう要請した。

①のマーケティング商品については、データブ

☆4 この法律は、与信、雇用、保険、住宅供給等の決定を下すために、信用報告機関が取り扱う消費者データの保護を定めており、FTC が法執行権限を有する。

☆5 利用者は、企業の重役、競争相手、昔のクラスメイト、友人、隣人などを探することができる。

事業の性質	データブローカは膨大な情報源からデータを収集し、その多くは消費者に認識されていない。
	データブローカ産業は複雑であり、データを相互に提供し合う複数レイヤのデータブローカが存在する。
	データブローカは、ほとんどすべてのアメリカの消費者を対象に、何十億ものデータ要素を収集、蓄積している。
	データブローカは、消費者に関する推測を行うために消費者に関するデータを結合・分析し、それには潜在的に機微な推測が含まれる。
	データブローカは、消費者にオンラインでの売り込みを行うために、オンラインおよびオフラインデータを結合する。
便益およびリスク	消費者は、なりすまし詐欺の防止や製品の品質向上、個人向け広告など、データブローカがデータを収集・利用する目的の多くから利益を得る。
	データブローカがデータを収集・利用する目的の多くは、それと同時に、リスク緩和商品 ^{☆7} の評価ミスによって、消費者が市場での信頼を失い、理由も分からずに取引を拒否されるなどのリスクをもたらす。
	消費者に関するデータを無限に蓄積することはセキュリティのリスクを生じさせる。
消費者の選択	データブローカが消費者のデータに関して消費者に与えている選択の程度では、かかる選択の多くは不可視的で不完全である。

表-3 データブローカに関する FTC の認識事項

ローカに対し、消費者が自らのデータにアクセスし、マーケティング目的での情報共有をオプトアウト^{☆6}できるように義務づけるべきである。アクセスできる対象には機微データも含めるべきである。また、消費者がこれらの権利を効果的に行使できるようにするために、立法によって、インターネットポータルのような中央化した仕組みの創設を義務づけることもあり得る。データブローカは、そこで自社を特定し、情報収集および利用の実務を説明し、アクセス手段およびオプトアウトのリンクを提供することができる。

さらに透明性を高めるために、データブローカに対し、たとえば自社の Web サイト上などで、情報源から取得した氏名、住所、年齢および収入の範囲といった生データ (実データ要素) を使うことのみならず、データから一定の推測を行うことにより生

☆6 事後的に拒否すること。

☆7 住所、氏名などの本人を確認する商品や、SSN が多数の住所と結び付いて利用されていないかを確認できる商品など。

じる派生データ（派生データ要素）を用いることを明確に消費者に開示するよう義務づけるべきである。派生データとは、たとえば、小型船舶免許を持つ人がボートに関心を持っている、ある消費者が「ワイヤード」誌を購読していることから技術に関心を持っている、ある消費者が Zappos.com のサイトを訪れたことから靴に関心を持っている、フォード車を2台買った消費者には同ブランドへのロイヤルティがあると推測するような場合を意味する。

消費者が自らのデータにアクセスできるようにすることは、健康情報に関するもののように、特に機微情報の場合には重要である。機微な消費者の嗜好および性質に関して推測を行う場合も同様である。

たとえば、消費者がオリジナルの公的記録源を用いて自らのデータを訂正する必要がある場合には、消費者がよりよく決断を下せるように、情報源の名前および／またはその類型を明確に開示するようデータブローカに義務づけるべきである。もちろん、この分野の立法は、個人消費者にアクセスを提供することの潜在的なセキュリティリスクと、かかるリスクを緩和する潜在的な手法を衡量すべきである。

消費者に対面する情報源に対しては、消費者データをデータブローカと共有することを目立つ形で消費者に通知し、データブローカとの情報共有をオプトアウトする能力のような選択を消費者に与えるよう義務づけるべきである。また、かかる情報源に対し、情報を収集しデータブローカと共有する前に、明示的な積極的同意を取得するよう義務づけることにより、健康情報のような機微情報への保護を与えるべきである。さらに、かかる情報源に対しては、データブローカが用意するアクセスおよびオプトアウトの権利を説明する中央化した仕組みへの情報またはリンクとともに、データを開示する先のデータブローカの名称を提供するよう義務づけるべきである。

なお、FTC は、現実には、消費者がアクセスを行使しないであろうことを認識しているが、立法化提案は、単に消費者への透明性を提供することに加え、他の主要な利害関係者——規制者、政策立案者、

学者、業界および消費者保護団体を含む——において、データブローカが自らの実務を消費者に明確かつ正確に説明しているか否かを評価するための説明責任を促進するであろうと説明している。

②のリスク緩和商品について、報告書は、携帯電話を契約する際の本人確認を行うケースのように、公正信用報告法が適用されない場合を含め、消費者が取引を行う能力を制限するリスク緩和商品を販売するデータブローカに対し、透明性を高める立法の必要性を勧告している。具体的には、(1) 消費者が取引を行いまは利益を得る能力に対してリスク緩和商品が悪影響を与える場合には、消費者と対面する企業は、企業が依存するデータを持つデータブローカを特定すること、(2) データブローカは、消費者に対し、利用される情報へのアクセス権を与え、適切な場合には誤った情報を訂正する権利を付与することが提案されている。ただし、不心得者に真実のデータを訂正されないようにするため、データの正確性および安全性を維持しつつ消費者のアクセスを可能にする方法を検討することが求められる。

③人探しについて、(1) 消費者が自らの情報にアクセスできるようにすること、(2) 消費者がかかる情報の利用を制限できるようにすること、(3) 可能であれば消費者が情報源でかかる情報を訂正できるようにするために、消費者にデータブローカの情報源を開示すること、(4) 近似する個人の氏名が検索結果に表示され続けるかもしれないという事実のように、オプトアウトの制限を明示的に開示することを勧告している。

以上のほか、報告書は、ベストプラクティスとして、PbD の導入、児童の保護、差別的な目的のためのデータ利用の禁止を実現するための措置を講じるよう、データブローカに勧告している。

立法化と政策動向

アメリカのプライバシーをめぐるここ数年の動きとしては、特に消費者プライバシー保護との関係で、ホワイトハウスの政策大綱や FTC の報告書が複数

公表されている。連邦法レベルでは、消費者プライバシー権利章典やセキュリティ侵害通知の立法化に向けた取り組みが注目される。州法レベルでは、カリフォルニア州が先進的な法律を制定し、中にはセキュリティ侵害通知法のように、国外に影響を与えるものもある。

データブローカ規制に関しては、透明性を担保するための立法化が提言されている。しかし、連邦議会の第113会期（2013～2014年）において、John D. Rockefeller IV が2014年2月12日に「データブローカ説明および透明性法案」(Data Broker Accountability and Transparency Act) を提出し、

カリフォルニア州でも同年2月21日に同種の法案が提出されたものの、同年8月末時点において、いずれも成立には至っていない。データブローカを取り締まるための立法例には、イギリスのように個人情報情報を不正に取得・提供する者を罰するものもあるが、アメリカは、データブローカの存在を認めつつ、透明性を高めるための立法化を指向している。

(2014年8月25日受付)

■石井 夏生利 kaoriish@slis.tsukuba.ac.jp
筑波大学図書館情報メディア系准教授。2007年中央大学大学院法学研究科国際企業関係法専攻博士後期課程修了。博士（法学）。2004年より、情報セキュリティ大学院大学助手、助教、講師、准教授を経て、2010年より現職。