米国における個人情報・プライバシー保護・活用の動向

和田恭@JETRO/IPA New York

1. はじめに

近年、簡便で莫大な情報蓄積場所を提供するクラウドコンピューティングや、様々な情報の容易なアップロードを可能とするモバイル端末・アプリケーションの普及により、ソーシャルメディアやオンライン販売を通じたコメント、閲覧・購買履歴などの個人情報がインターネット上により多く集積されるようになってきている。

これらの情報の活用により、個人間のコミュニケーションが促進され、事業者サイドからはきめ細かな個人向けのサービスが可能になる一方で、消費者の意識しない間に情報が収集される場面が増えたり、情報をアップロードした者が意図しない形で、個人情報が伝播・共有され、場合によっては悪意ある第三者の手に渡ったりといった個人情報の漏えい・不正利用、プライバシーの侵害といった問題を引き起こす可能性も増大している。

米国内では、これに対して、「消費者プライバシー権利章典」の起草や、インターネットアクセスを通じた消費者行動の追跡を行わせない Do Not Track 条項を含むオンライン自主規制ガイドラインの制定など、インターネット上のビジネスに関し、個人に関する情報に対する規制・訴訟などのリスクを減らし、積極的にビジネス展開が行える環境整備をすすめようとする動きが出てきている。

以上の問題意識をもとに、本稿では、米国の連邦政府及び IT 業界における個人情報・プライバシー情報の保護と活用の取り組みについて報告する。

2. 米国での個人情報・プライバシーの取り扱いを巡る現状

本章では、米国における個人情報[1]・プライバシー保護に関する枠組み、情報漏えいの状況やその影響、個人情報を取り扱うサービス形態などを紹介する。

(1) 個人情報・プライバシー保護に対する基本的な考え

米国ではプライバシーの保護について、合衆国憲法修正第 4 条において、「不合理な捜索及び逮捕押収に対し、その身体、住居、書類及び所有物の安全を保障される国民の権利は、これを侵してはならない。令状はすべて、宣誓又は確約によって支持される、相当な理由に基づいて発せられ、且つ捜索されるべき場所及び逮捕押収されるべき人又は物を特に記載したものでなければ、これを発してはならない」と定めている。一般的には、プライバシーについては、理念的に「他にわずらわされることなく一人で放置してもらう」という古典的な考え方や、「自己に関する情報の取り扱いは自分で決定できる」という考え方が存在するが[2]、同条の解釈として、個人に関する情報がどう取り扱われるべきかについては見解が分かれている。

米国民の個人情報・プライバシー保護に関する関心は、最近の関連訴訟をみる限りは、自己に関する情報がどのように利用されるかの事前承認・事後コントロール権が確保できているか否かについてであり、とりわけ、警察などの公権力から（企業が集積した）個人の情報がどう保護されるかについてはセンシティブなようである。

そのような事情もあってか、連邦レベルでの包括的な個人情報保護法・プライバシー保護法は存在せず、州法を除けば、医療関係の個人情報保護を規定した Health Insurance Portability and Accountability Act やオンラインによる 13 歳未満の青少年の個人情報収集を制限する Children's Online Privacy Protection Act など分野別または特定政策目的のための規正法が存在するにとどまっている。（個人情報保護関係法令については後述。）

総じてこれまでは、個人情報･プライバシーの取り扱いは、業界・企業のビジネス上の取組みが先行し、何か問題が生じた場合に業界自主規制や民事損害賠償による解決を行うという流れが主となっていた。しかし、スマートフォン・タブレットなどモバイル端末による画像・位置情報のアップロードなどによって様々な個人の行動履歴（ライフログ）がインターネット上に蓄積されるようになった現在、いわゆるビッグデータ分析などそれらの個人

[1] 米国では、個人情報は Personal Identifiable Information (PII)と呼ばれているが、わが国の「個人情報保護法」に基づく「個人情報」のような明確な定義はない。本稿では、「個人情報」を「個人を特定可能な情報」、「プライバシー情報」を「自己に関するものとして、他者に対して一定の取り扱いを要求できる情報」との意味で用いている。
[2] http://www.hogen.org/research/paper/lj24/index.html

情報・プライバシー情報を利用する新たなビジネスが急速に成長しつつあり、その阻害要因となる規制・訴訟リスクを最小限化することが求められている。

2012 年 2 月 23 日、大統領府は、個人情報・プライバシー情報の保護とインターネット活用促進に向け、「我々は、もう待てない」とのキャッチフレーズとともに「プライバシー権利章典（Privacy Bill of Rights）」の草案を発表した。本章典は、以下の項目からなる。

- 個人によるコントロール：消費者は、個人情報を利用する事業者に対し、自己の情報をコントロールする権利を有する
- 透明性：消費者は、プライバシーとセキュリティの遵守方法に関して分かりやすい説明を受ける権利を有する
- 背景事情の尊重：消費者は、自己の情報が収集、利用、公開される際に、それを提供した際の背景事情に沿って行われるよう配慮される権利を有する
- セキュリティ：消費者は、個人情報が安全で責任のある取り扱いを受ける権利を有する
- アクセスと正確性：消費者は、情報の機微度合いと不正確だった場合の不利益にかんがみ適切な方法で、個人情報にアクセス、修正する権利を有する
- 合理的な範囲での情報収集：消費者は、事業者が収集、保持する個人情報について合理的な範囲に制限する権利を有する
- 説明責任：消費者は、消費者プライバシー権利章典に準拠するために適切な方法により、個人情報の取り扱いを受ける権利を有する

この章典では、オンライン小売事業者などが消費者のインターネット上の行動を追跡することを拒否できる権利（「Do Not Track」）の制度化や、子供に対するオンライン上のプライバシー保護強化など、最近のインターネット利用におけるプライバシー上の課題に機動的に対応する内容となっている。また、同章典では、あわせて、①ステークホルダーによる同章典のビジネス分野への適用方策の検討、②連邦取引委員会（FTC）による規制活動の強化、③同章典の法制化に関する議会への働きかけ、④個人情報の取り扱いに関する国際的な相互運用性の確保などの取組みを進めることとされている。

一方、EU においても個人情報保護は強化の方向にある。EU では個人情報保護に関する EU 指令が 1995 年に発効しており、これを受けて域内各国で個人情報保護規制が施行されているところである。しかし、27 カ国での施行形態がばらばらであることや、技術とグローバリゼーションへの対応が必要との認識から、欧州委員会（European Commission）は、2012 年 1 月 25 日、個人情報の保護体系の見直しに着手することを

発表している[3]。また、米国との間でも、本章典の起草を契機として、積極的に調整に入っている。2012 年 4 月 19 日の US-EU 共同声明では、グローバルに個人情報の保護が可能となるよう国・地域間での情報保護体制の相互承認枠組みを構築すること、それぞれの域内において統一的な個人情報保護体制を徹底すること、昨今のプライバシー保護に関する課題について国際的な取組みを行うことなど、今後の個人情報保護に向けた国際協力の方向性が打ち出された[4]。

もともと、EU 指令では、適切な個人情報保護体制をとっていない国へのデータ提供を禁止しているが、連邦政府レベルでの個人情報保護法をもたない米国へのデータ移動を可能とするため、US-EU 間でのセーフハーバー枠組みを 2000 年に締結している[5]。同枠組みに基づき、米国内企業は、商務省に個人情報保護に関する EU 指令の遵守を申告することにより、EU 指令を遵守しているとみなされ、EU とのデータ交換を可能となるのであり、上述の US-EU 間の共同声明においても、引き続いて同枠組みを活用していくことがうたわれている。

(2)　個人情報漏えいに関する状況

個人情報保護強化の動きとはうらはらに、個人情報漏えいに関する事例は後を絶たない。米国の個人情報窃盗被害等の調査機関 Identity Theft Resource Center(ITRC)によれば、ここ数年の業種別の個人情報漏えい事例の発生状況は以下のとおりである。個人情報の漏えいやプライバシーの侵害が発生した際に政府又は民間レベルで必要な対応（損害賠償請求を含む）が取れるよう、HIPAA 法施行規則や州法において、個人情報を取り扱う事業者に対し当局に事例発生の通報が義務付けられており、本調査では、それら法令に基づく通報や ITRC に対する通報などが集計されている。なお、漏えいしたレコード数（＝のべ人数）は年によって大きく異なるが、2011 年では 2,292 万件であった。

【表 1：米国の個人情報漏えい事例発生件数の推移[6]】

分野	2008 年	2009 年	2010 年	2011 年
金融	78 (12%)	57 (11.4%)	54 (8.1%)	28 (6.7%)
ビジネス	240 (36%)	208 (41.8%)	279 (42.1%)	198 (47.3%)
教育	131 (20%)	78 (15.7%)	65 (9.9%)	59 (14.1%)
政府・軍	110 (17%)	90 (18.1%)	104 (15.7%)	48 (11.5%)
医療	97 (15%)	65 (13.1%)	160 (24.1%)	86 (20.5%)
合計	656 (100%)	498 (100%)	662 (100%)	419 (100%)

[3] http://ec.europa.eu/justice/newsroom/data-protection/news/120125_en.htm
[4] http://www.commerce.gov/news/press-releases/2012/03/19/us-eu-joint-statement-privacy-eu-commission-vice-president-viviane-re
[5] http://export.gov/safeharbor/eu/index.asp
[6] http://www.idtheftcenter.org/artman2/publish/lib_survey/ITRC_2008_Breach_List.shtml
に基づき筆者作成。

対象となる「個人情報」の定義や事例発生についての通報義務の有無が異なるため、直接的な比較はできないが、わが国の情報漏えい事例発生件数は、NPO 日本ネットワークセキュリティ協会（JNSA）によると年間 1,000~1,600 件程度、漏えいレコード件数は 2010 年で 558 万人であった[7]。わが国では金融及び政府部門の情報漏えい事例が多いが、米国では、ビジネス及び医療部門の件数が多いのが特徴といえる。

以下では、過去の特徴的な個人情報漏えい事例に加え、ソーシャルメディアや各種モバイル端末の普及に伴い、個人情報のオンライン共有が盛んとなった最近 2～3 年間を中心に、米国で個人情報の漏洩やプライバシーの侵害が問題となった事例について紹介する。

【図表 2: 主要な最近の個人情報漏えい・プライバシー侵害事例】

事案	時期	概要	結果
DoubleClick 社によるオンライン行動トラッキング問題	2000～2002 年	California 州在住の女性が、DoubleClick 社によるオンライン行動トラッキング目的の Cookie ファイル配布行為によりプライバシーを侵害されたとして、同社を提訴[8]。	DoubleClick 社は、プライバシーポリシの明確化、プライバシー保護に関する啓蒙活動の展開、Cookie からのオプトアウト方法提供、などを条件に原告と和解[9]。
Heartland Payment Systems 社に対するサイバー攻撃	2008 年	クレジットカード決済処理事業者の Heartland Payment Systems 社システムにハッカーが不正アクセスし、約 1 億 3,000 万件のクレジット・デビットカード番号が盗難される[10]。	クレジット･でビットカード番号の不正使用などにより、推定約 2 億ドルの被害が発生。首謀者は逮捕され、禁固 20 年の判決を受ける[11]。
Facebook Beacon に関する問題	2007～2009 年	Facebook 社のパートナー企業（当初 44 社）ウェブサイト上における訪問者の行動が、Beacon と呼ばれる仕組みを介して Facebook 社に送信されていたことが問題化[12]。	ユーザーからの懸念や複数の訴訟を受け、Facebook 社は 2009 年に Beacon を廃止[13]。
Google Buzz の	2010 年	Google 社の SNS「Buzz」（現在	プライバシー侵害を理由とする集

[7] http://www.jnsa.org/result/incident/data/2010incident_survey_PIL_v1.4.pdf
[8] http://www.theregister.co.uk/2000/01/28/doubleclick_sued_over_alleged_cookie/
[9] http://epic.org/privacy/internet/cookies/dblclkproposedsettlement.pdf
[10] http://www.2008breach.com/Information20090120.asp
http://www.wired.com/threatlevel/2009/08/tjx-hacker-charged-with-heartland/
[11] http://www.pcmag.com/article2/0,2817,2361854,00.asp
[12] https://www.pcworld.com/article/140182/facebooks_beacon_more_intrusive_than_previously_thought.html
[13] http://www.theregister.co.uk/2009/09/23/facebook_beacon_dies/

プライバシー設定に関する論議		は廃止）において、初期設定ではBuzz ユーザーの連絡帳[14]情報のうち一部が一般公開されるようになっていたことが問題化[15]。	団訴訟を受けた Google 社は、オンラインプライバシーについて啓蒙する団体を支援することで原告団と和解。連邦取引委員会（Federal Trade Commission、FTC）は、同社により Buzz ユーザーのプライバシーが侵害されたと断定、今後 20 年にわたり同社のプライバシー遵守状況の監査実施などで和解した[16]。ユーザー利用の低迷により同社は Buzz を 2011 年に廃止。
Google Street View 撮影車両によるデータ不正収集問題	2010 年	街路の写真を撮影し、無料公開するサービス「Street View」において、撮影車両が、パスワード保護されていない車両周辺の WiFi ネットワーク上で交信されるデータを無断で収集、保存していたことが問題化[17]。	各国の司法当局から行政指導などを受けた Google 社は、WiFi ネットワーク上で交信されるデータの収集を 2010 年に停止[18]。
ソニーに対するサイバー攻撃	2011 年	ソニー運営のゲームネットワーク「PlayStation Network（PSN）」に対して何者かが不正アクセスし、約 7,700 万件のアカウント情報が盗難される[19]。	連邦議会における証人喚問に発展。ソニーは、PSN 加入者に対して複数のゲームなどを無償提供するとともに、被害補償保険加入などを表明。更に、PSN 利用規約を変更し、「今後 PSN からデータ漏洩が発生した場合も、ユーザーはソニーを提訴できない」という旨の文面を追加[20]。
Carrier IQ に関する問題	2011 年	米国で販売されている多数のスマートフォン上に、ユーザーによ	キャリアおよび端末メーカー各社は、販売・製造端末の Carrier IQ

[14] 同じく Google 社が提供する電子メールサービス「Gmail」の連絡帳。
[15] https://www.pcworld.com/businesscenter/article/189081/google_buzz_criticized_for_disclosing_gmail_contacts.html
[16] http://www.ftc.gov/opa/2011/03/google.shtm
http://www.webcitation.org/5tyF08T40
http://itpro.nikkeibp.co.jp/article/NEWS/20111025/371324/
[17] http://www.zdnet.com.au/google-admits-to-wi-fi-spying-339303194.htm
[18] http://searchengineland.com/google-ends-street-view-wifi-data-collection-potentially-needs-other-sources-for-location-53373
[19] http://www.telegraph.co.uk/technology/news/8475728/Millions-of-internet-users-hit-by-massive-Sony-PlayStation-data-theft.html
[20] http://www.bbc.co.uk/news/technology-14948701
http://kotaku.com/5804318/
http://blog.us.playstation.com/2011/05/14/ps3-system-software-update/
http://www.eurogamer.net/articles/2011-05-01-psn-sony-outlines-welcome-back-gifts

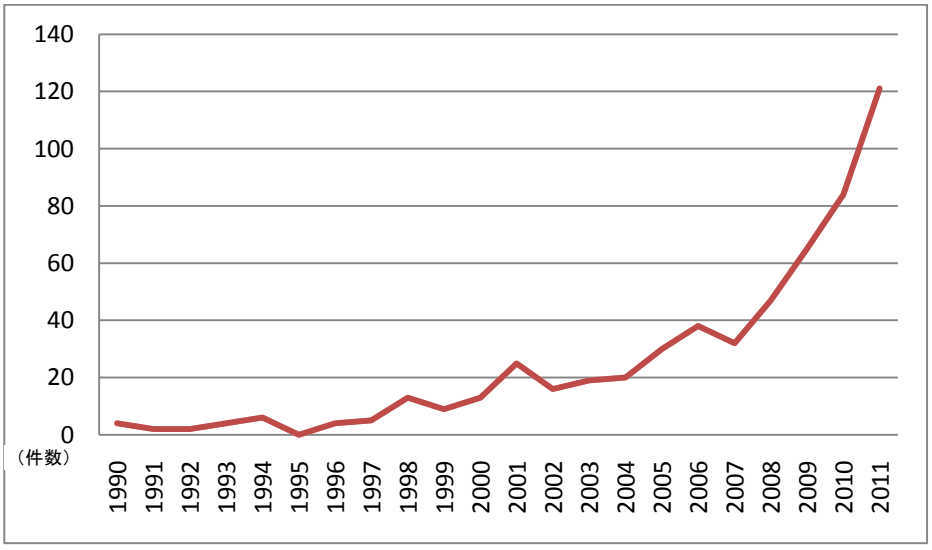
		るスマートフォン操作を記録するソフトウェア「Carrier IQ」がユーザーの許可無しに事前搭載されていることが発覚し、問題化[21]。	搭載有無を公開の上、同ソフトウェア搭載の理由や同ソフトウェアにより収集されるデータの種類について説明。一部の端末メーカーは今後 Carrier IQ を搭載しない意向を表明[22]。
Facebook 社の個人情報取り扱いに関する FTC との争議	2009～2011 年	Facebook 社が、ユーザーの許可無くユーザー情報を第 3 者（広告主など）と共有していたとして、FTC が調査[23]。	Facebook 社は、第 3 者とのユーザー情報共有前に明確な形でユーザーの承諾を得ること、および向こう 20 年間、2 年毎に独立機関による監査を受けることを条件に、2012 年、FTC と和解[24]。
Global Payments 社に対するサイバー攻撃	2012 年	クレジットカードなど電子決済処理事業者の Global Payments 社システムにハッカーが不正アクセスし、アカウント情報約 5 万～1,000 万件が盗難された[25]。	Global Payments 社は、漏洩被害に遭ったアカウント数は 150 万以下と発表。また、いくらかのクレジットカード番号が漏洩したものの、氏名、住所、社会保障番号（Social Security Number、SSN）は漏洩しなかったと主張[26]。
Google 社プライバシーポリシ変更に伴う論議	2012 年	Google 社が、同社が運営する複数のサービスにおけるユーザー情報を一元化し、広告表示やパーソナライズ目的などに利用できるよう、プライバシーポリシを変更したことが問題化[27]。	欧州連合（EU）各国の当局は、同社の新規プライバシーポリシの合法性について懸念を表明。複数の Google 社サービス利用者は、新規プライバシーポリシが違法であるとして同社を提訴[28]。
RockYou 社に対するサイバー攻撃	2009～2012 年	ソーシャルゲーム開発企業 RockYou 社システムにハッカーが不正アクセスし、アカウント情報約 3,200 万件が盗難された。また、パスワードなど機敏なユーザー情報が暗号化されないまま	FTC より調査を受けた同社は、25 万ドルの罰金や、セキュリティ対策の強化と維持などを条件に、2012 年、FTC と和解[30]。

[21] http://www.wired.com/threatlevel/2011/11/secret-software-logging-video
[22] http://www.macworld.co.uk/ipad-iphone/news/?newsid=3322441
http://www.computerworld.com/s/article/print/9222319/AT_T_Sprint_confirm_use_of_Carrier_IQ_software_on_handsets
[23] https://www.nytimes.com/2011/11/30/technology/facebook-agrees-to-ftc-settlement-on-privacy.html
[24] https://www.nytimes.com/2011/11/30/technology/facebook-agrees-to-ftc-settlement-on-privacy.html
[25] http://www.bloomberg.com/news/2012-03-30/global-payments-trades-halted-as-card-firms-probe-breach.html
[26] http://articles.latimes.com/2012/apr/02/business/la-fi-visa-breach-20120402
[27] http://news.cnet.com/8301-13506_3-57388415-17/googles-new-privacy-policy-begins-does-it-break-the-law/
[28] http://news.cnet.com/8301-27080_3-57402965-245/google-users-sue-over-changes-to-privacy-policy/
http://news.cnet.com/8301-13506_3-57388415-17/googles-new-privacy-policy-begins-does-it-break-the-law/

		同社システムに保存されていたことなどが問題化[29]。	
Google v Safari	2012 年	Google 社が、Apple 社製ウェブブラウザ「Safari」ユーザーのプライバシー設定を迂回し、設定に関係なく Safari ユーザーをトラッキングできる仕組みを開発、展開していたことが問題化[31]。	FTC は Google 社に対する調査を開始。2012 年 5 月現在未決着であるものの、FTC は同社に対して約 1,000 万ドルの罰金を課すとの見方が優勢。

全体的に個人情報に関する盗難・犯罪の増大、消費者の権利意識の高まりなどを反映して、個人情報・プライバシー情報関係の訴訟も増大の一途にある。1990 年以降に連邦及び各州において起こされた情報漏えい関連の訴訟のうち、判決に至ったものの推移は以下のとおりである。

【図表 3：1990 年以降の情報漏えい関連判決件数の推移[32]】



漏えいレコード数（＝のべ人数）でみても、情報漏えい事例の規模は増大の一歩をたどっている。個人情報・プライバシー保護に向けた啓蒙活動を展開する非営利団体 Privacy

[30] https://www.pcworld.com/article/252725/rockyou_settles_pending_charges_for_250k_over_data_breach.html
[29] http://techcrunch.com/2009/12/14/rockyou-hack-security-myspace-facebook-passwords/
[31] http://www.theverge.com/2012/5/4/2999451/google-ftc-fine-safari-cookie-tracking
[32] McDermott Will & Emery LLP 調査データに基づき作成。 Computer Fraud and Abuse Act、Stored Communications Act”、Electronic Communications Privacy Act、Wiretap Act に関する全判決件数を合計。

Rights Clearinghouse（PRC）によると、2005 年以降の情報漏えい全事例中、レコード数の大きいものは以下のとおりである。

【図表 4：米国における情報漏えいレコード数 11 大事例[33]】

	発見日	漏えい発生企業	本拠地	漏洩レコード数
1	2009/1/20	Heartland Payment Systems	ニュージャージー州	130,000,000
2	2007/1/17	TJX (TJ Max, Marshall's 等を含む小売チェーン)	マサチューセッツ州	100,000,000
2	2010/1/1	Netflix	カリフォルニア州	100,000,000
4	2009/10/2	U.S. Military Veterans	ワシントン DC	76,000,000
5	2005/6/16	CardSystems	アリゾナ州	40,000,000
6	2006/5/22	U.S. Department of Veterans Affairs	ワシントン DC	26,500,000
7	2012/1/15	Zappos.com	カリフォルニア州	24,000,000
8	2011/4/11	Word Press	カリフォルニア州	18,000,000
9	2008/8/2	Countrywide Financial Corp.	カリフォルニア州	17,000,000
10	2008/3/26	Bank of New York Mellon	ペンシルベニア州	12,500,000
11	2011/4/27	Sony PlayStation Network, Sony Online Entertainment	ニューヨーク州	12,000,000

これらの情報漏えいがもたらす企業イメージへの影響は大きい。ソニーPlayStation Network の事例は記憶に新しいが、米国過去最大の Heartland Payment Systems 社の事例では、毎月およそ 1 億件の決済データを処理する同社のサーバーへのハッカー侵入により大量の個人データが漏えいし、2010 年に VISA と 6 千万ドル、MasterCard と 4,140 万ドルなどといった巨額の和解金を支払わざるを得なくなり、同社の株価は発覚当時の 14ドルから 2009 年 3 月には 4ドル前後まで低迷したといわれている[34]。

なお、以上に示したデータは、あくまでも漏えいの事実が公表されたものに限定されており、公にならなかった事例も含めると、これをはるかに上回る量の個人情報・プライバシー情報が漏えいしているものと考えられる。更に、受動的な形での個人情報漏えいケース（例えば、Facebook にアップロードしたデータのプライバシー設定を誤ったために、友人のみに公表する意図のデータが一般公開されてしまうケース、など）も多数存在することから、上表に示される漏えい件数はあくまでも氷山の一角に過ぎないと考えられる。

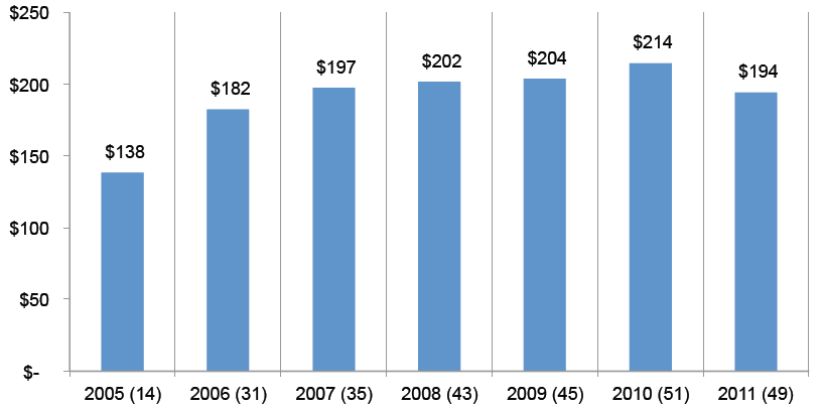
次に、参考情報として、Symantec 社が PonemonInstitute 社への委託により行った調査によれば、データ（個人情報、個人情報以外の機密情報問わず）漏えいによる米国企業への被害規模（1 社当たり）推移は以下のとおりである。

[33] http://www.privacyrights.org/data-breach の全データに基づき作成。なお、ソニーの事例は漏えいレコード総数 1.1 億件中、暗号化されておらず「個人情報の漏えい」としてカウントされた件数のみを掲載している
[34] http://www.finextra.com/news/fullstory.aspx?newsitemid=21753

【図表 5: データ漏えいによる米国企業(1 社当たり)の被害額推移(単位:100 万ドル)[35]】

また、企業からデータが漏えいした場合の、漏えいデータ 1 件当たりの米国企業に対する被害額推移は以下のとおりとなっている。

【図表 6: データ漏えいによる米国企業(1 社当たり)への被害額(漏えいデータ 1 件当たり)推移

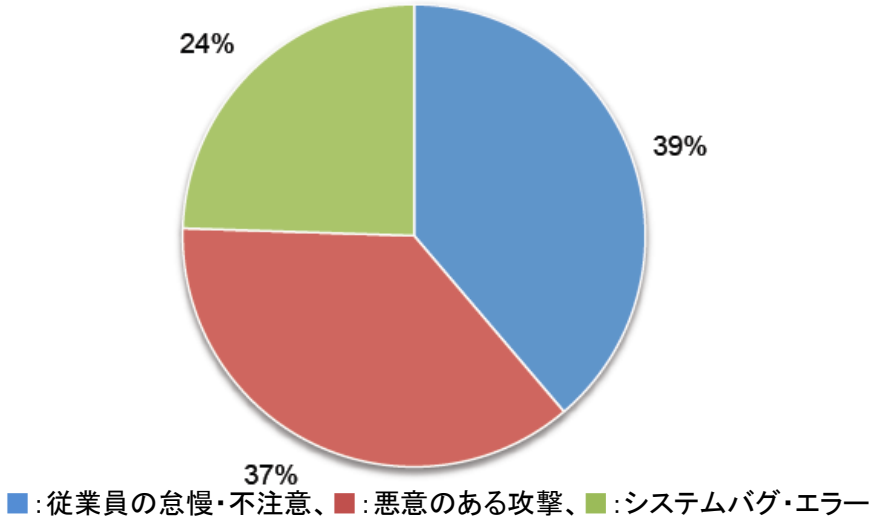


ここで、データ漏えいによる 1 社当たりの被害額、漏えいデータ 1 件当たりの被害額ともに、2005 年から 2010 年にかけて毎年上昇した後、2011 年には減少に転じている。2011 年になって被害額が減少した明確な理由は明らかになっていないが、同調査において、企業からのデータ漏えいの原因も分析されており、データ漏えいのうち、悪意ある攻撃によるものが 37%で、2008 年度比(12%)で 3 倍になっているものの、依然としてその大半の 63%が企業側の責任によるもの(従業員の怠慢とシステムバグ)であるこ

[35] http://www.symantec.com/content/en/us/about/media/pdfs/b-ponemon-2011-cost-of-data-breach-us.en-us.pdf
図中、括弧内の数字は調査対象となった企業の数を示す。次表も同じ。

とが分かる。これを前提とすれば、従業員の意識やシステムの堅牢性が全体的に向上したことが、2011 年に入って、被害額の減少（1 社あたり、漏えいデータ 1 件当たり）につながった可能性があると考えられる。

【図表 7：米国企業におけるデータ漏えいの原因】



(3)　個人情報・プライバシー保護に関する消費者意識

ソーシャルメディアや、スマートフォンの利用が急速に拡大しているが、米国の消費者の個人情報保護やセキュリティ確保についての関心が鈍化しているわけではない。Anonymizer 社が 2011 年 10 月に発表した調査結果によれば、米国の Facebook ユーザーのうち、56%は、ソーシャルメディアの利用はプライバシーの侵害につながると認識しているとのことである[36]。

プライバシー保護に対するコスト意識の一例として、Frog design 社が 2011 年に行った「特定の種類の個人情報を保護するサービスに対して、毎年何ドルまで支払ってもよいか」を問う調査結果を紹介する[37]。

[36] http://markets.financialcontent.com/stocks/news/read/19770061/New_Survey_Finds_Consumers_Are_Cautious_About_Being_Online_But_Need_More_Vigilance_When_Protecting_Privacy
[37] http://designmind.frogdesign.com/blog/what039s-your-personal-data-worth.html

【図表 8: 米国消費者が個人情報保護のために毎年支払ってもよいとする金額（個人情報種類別）[38]】

以上の調査結果では、SSN や公式の ID といった、犯罪に悪用されれば被害が甚大な機微情報についての許容金額が最も高額（240 ドル/年）となっており、これにクレジットカード情報（150 ドル/年）、電子的な情報交信記録（チャットログ、SMS、電子メールなど）（59 ドル/年）、ウェブ検索記録（57 ドル/月）、位置情報記録（55 ドル/月）、ウェブ閲覧記録（52 ドル/月）、健康情報（38 ドル/月）が続く状況となっている。

以上から、企業における情報漏えいの損害額が 194 ドル/年・レコードという数字と合わせ、200～300 ドル程度が、米国の消費者・企業が認識する「個人情報の価値（あるいは損害賠償額）」なのではないかと考えられる[39]。なお、わが国における個人情報漏えいの損害賠償額は、（独）情報処理推進機構が 2012 年 3 月に発表した報告書「つながる IT がもたらす豊かなくらしと経済　～ビッグデータの価値と信頼～」によると、個々のケースで 500 円から 1 万 5,000 円と異なるが、目安として 1 万円/人程度とされている[40]。

この金額が高いか低いかは一概には言えないが、個人情報・プライバシー情報の保護はただではないという認識は、米国消費者にも確実にある。一方で、よりよいサービスが

[38] 回答者の 50%が「支払ってもよい」と意志表示した金額を表示。
[39] 当然のことながら、情報を保護するためのコストと、活用したい情報の入手コストは異なる。例えば、Facebook 社による Instagram 社買収は、後者のユーザー（2,700 万人、2012 年 1 月時点）を獲得するために 100 億ドルを投じたとの報道もあり、この事例について 1 月時点のユーザー数で単純計算すると Instagram ユーザーを入手するために Facebook が投じた投資価値は約 666 ドル/人となる。
[40] http://www.ipa.go.jp/about/research/2011bigdata/pdf/120330_bigdata.pdf
http://itpro.nikkeibp.co.jp/article/COLUMN/20110412/359332/?SS=imgview&FD=-1715429006&ST=selfup

受けられる、報酬が得られるといったトレードオフにより、消費者は気軽に個人情報を提供するということも知られている。

例えば、Facebook ではユーザー間のコミュニケーション手段として人気を博している反面、ユーザーが個人情報を過度にアップロード、共有している傾向にあることが指摘されている。例えば、Consumer Reports 2012 年 6 月号によると、米国内で、Facebook 上で家族のプロフィール、写真を自分のページ上に掲載しているユーザー数 3,930 万人、自分の誕生日（年）をプロファイル上公開しているユーザー2,040 万人、自分の健康状態や治療に関する情報に「like」を表示するユーザー470 万人などとされている。Facebook というサービスを円滑に利用するために、プライバシーの問題を認識しつつも、プライバシー情報を載せてしまうユーザーがいかに多いかが分かる。

ソーシャルメディアのユーザー/非ユーザーを比較すると、プライバシー保護に関する受容性が異なることも知られている。先述の Anonymizer 社の調査では、65%のユーザーが Facebook 利用はプライバシー侵害につながるとしている一方で、29%の利用者は利用をやめるつもりはないという結果が出ている。これは、ソーシャルメディアユーザーが、プライバシー保護の必要性を認識しなくなってきていることにも起因していると考えられる。MSNBC の消費者レポーターBob Sullivan 氏の調べによると、5 年前との比較で、ソーシャルメディアユーザーはプライバシー保護の必要性を認識しなくなってきているが、非ユーザーは認識がそう変わっていないことと対照的である。

【図表 9：5 年前と比較したプライバシー保護の必要性の変化】

Do you have more or less control over personal information today than five years ago?	Overall (percent)	Active social network user	Not active user
More	13	16	12
The same	18	18	18
Less	69	66	71

また、参考情報として、EU の消費者を対象に、「ウェブ上で製品・サービスを購入する際に、①購入者の個人情報は一切第 3 者と共有しない代わりに、商品の通常価格に 50 ユーロセント（約 64 セント）上乗せする小売業者、②電話番号または電子メールアドレスといった個人情報を第 3 者と共有するが、通常価格で商品を販売する小売業者、のどちらを選択するか」を問う調査も行われている。これによると、①を選択した回答者は全体の約 3 分の 1 に留まった、という結果が得られており、上述の調査結果とは反対に、消費者は一般的に個人情報保護サービスに対する出費を惜しむ傾向がある、との意見も見られている[41]。

[41] http://moneyland.time.com/2012/03/19/were-total-cheapskates-when-it-comes-to-our-privacy/

また、ソーシャルメディアでは様々なプライバシー情報がアップロードされる状況を背景に、企業において、従業員のソーシャルメディア活動を監視したり[42]、新規採用に当たり採用応募者のバックグラウンドチェックにソーシャルメディアを利用する事例が拡大している。中には、プライベートに関する情報を入手するため、採用応募者にソーシャルメディアのログイン情報を要求する事例が増加しているとのことである。これに対して、労働者保護などの観点からこうしたパスワード開示要求を禁止する条例が 2012 年 5 月にカリフォルニア州上院で可決したところであり、同様の動きが他の州や連邦政府議会にも広がっているとのことである[43]。

プライバシー保護について特段の配慮が必要とされる青少年対策についても、様々な議論がある。わが国でも、ソーシャルネットワーキングの未成年利用について、ネット上のいじめや犯罪被害に遭遇する可能性が高いことが問題になっているが、状況は米国でも同様である。例えば、Facebook では 13 歳未満のユーザーの利用を禁止しているが、これにも関わらず、登録年齢を偽ることにより参加するユーザーが後をたたず、2011 年時点で 13 歳未満のユーザーが 750 万人、10 歳未満のユーザーが 500 万人以上いるとされている[44]。Facebook 社はプライバシー遵守状況について、今後 20 年間の監査を受けることで FTC と合意したばかりであり、この状況を放置するわけにいかず、例えば親の管理下に置くことで子供のアクセスを許可するか、一定の機能制限をかけるなどの方法により、子供向けに一定の Facebook サービスを提供することを検討中であると伝えられている。

(4) 個人情報保護・利活用サービスの現状

近年、いわゆるビッグデータ分析をはじめとして、個人情報を利用、分析することにより、様々なサービスを生み出そうとする動きが加速してきている。米国では、個人情報の保護を代行するサービスや、個人情報の商用利用と引き換えに、該当個人に対して対価を支払う個人情報利活用サービスなども登場しており、ここではその代表的な事例を紹介する。

[42] ガートナーによれば、ソーシャルメディア上の社員行動を監視する企業の割合は 2015 年に 60%に上るとのことである。
http://www.gartner.com/it/page.jsp?id=2028215
[43] http://www.computerworld.com.au/article/424340/california_moves_stop_employers_demanding_facebook_passwords/
[44] http://online.wsj.com/article/SB10001424052702303506404577444711741019238.html

【図表 10：米国における個人情報保護・利活用サービス例】

サービス種別	概要	代表的な事業者名
個人情報アグリゲーション・ブローカーサービス	SNS、コンテンツ共有サイト、コミュニティサイト、その他公開情報など、一般公開されている個人情報を収集し、有料で検索できるようにしたり、広告主など第 3 者に販売するサービスを提供。一般的に、各個人に対する報酬や対価はなし。多くの事業者はデータ削除要求に応じるが、申請方法が複雑な場合、削除費用を課金する場合などもある[45]。	• Intelius • BeenVerified • Spokeo • Anywho • Scopeo • White Pages • ZoomInfo • MediConnect Global
個人情報価値評価サービス	Twitter や Facebook といった SNS 上アカウントの金銭価値を評価するサービス。フォロワー数、友人数、投稿コンテンツ共有数などといった指標をベースに、各アカウントの価値を算出する。	Klout
公開個人情報の削除代行サービス	個人情報アグリゲーションサービスやブローカーサービス事業者に対して、データ削除申請を消費者に代わって行うサービス。	• Reputation.com • Abine
個人情報不正使用のモニタリングサービス	第 3 者による個人情報の不正使用（なりすまし、身元詐称など）を防止するため、消費者に代わってウェブ上での個人情報使用状況を監視するサービス。	• CSIdentity • LifeLock • Intelius • Reputation.com
データロッカーサービス	消費者の任意入力による各種個人情報を保存し、特定の目的において個人情報が必要とされる場合に、必要な種類の個人情報のみを抽出し、要求者に対して共有するサービス。共有時に消費者に対して対価を支払うことを想定する動きもある[46]。	• Singly • Connect.me • Personal.com • The Locker Project

[45] https://www.privacyrights.org/online-information-brokers-and-consumer-privacy
[46] http://www.huffingtonpost.com/2011/05/06/reputationcom-ceo-personal-information_n_858485.html

3. 民間における個人情報・プライバシー保護の取り組み

個人情報・プライバシー保護意識の高まりを受け、一般企業や業界団体による個人情報・プライバシー保護を強化するための標準化、自主規制、ガイドライン制定といった動きもある。以下では、これらの企業・団体による取り組み状況について紹介する。

(1) 標準化活動

① ISMS（Information Security Management System）

情報セキュリティ管理体制（セキュリティポリシー、ポリシーの遂行方法、システム）についての理念を形容する概念として、情報セキュリティマネジメントシステム（Information Security Management System、ISMS）という仕組みが存在する。ISMS は、大枠には PDCA（Plan-Do-Check-Act）サイクルとよばれる品質管理プロセスの実行を想定するものであり、同プロセスの概要は以下の通りである[47]。

- Plan（計画）: セキュリティリスクを識別し、リスクに対応するための適切なシステム要件を設定すること。
- Do（実行）: システム要件を満たすための対策や仕組みを導入すること。
- Check（確認）: システム要件が十分に満たされているかどうか確認すること。
- Act（変更・修正）: Check の結果、必要に応じてシステム内容を変更すること。

これに基づき、ISO/IEC 27001 ほかの国際規格が制定されているが、米国で ISMS 規格の認証取得活動はそれほど活発とはいえない。これに対し、わが国では、ISMS 規格認証に加えて、個人情報保護法の制定等を受け、「個人情報保護マネジメントシステム（JIS Q 15001）」が別途制定されており、同規格への適合性評価をおこなう「プライバシーマーク制度」が一般財団法人日本情報経済社会推進協会（JIPDEC）により運営されている[48]。

② PCI-DSS（Payment Card Industry Data Security Standard）

個人情報体制に関するものではないが、情報漏えい防止の観点から、決済関連の標準を紹介する。大手クレジットカード会社 5 社（Visa 社、MasterCard 社、American Express 社、Discover 社、JCB 社）により、決済カード業界データセキュリティスタンダード（Payment Card Industry Data Security Standard、PCI-DSS）が 2004 年 12 月に策定されている[49]。この PCI-DSS は、2010 年 10 月に新版であるバージョン 2.0 の

[47] http://openlearn.open.ac.uk/mod/oucontent/view.php?id=397613&section=7
[48] http://privacymark.jp/privacy_mark/about/outline_and_purpose.html
[49] http://arielsilverstone.com/pci-security/the-coming-storm-pci-dss-2-0/

草案が公表されており、約 1 年の猶予期間を経て、2012 年 1 月には同バージョンが発効している。

ただし、近年大規模なサイバー攻撃の被害に遭った Heartland Payment Systems 社や Global Payments 社（上述）は、いずれも攻撃発生時に PCI-DSS 準拠を名乗っていた経緯があるように、同規格への準拠が必ずしも完全なセキュリティリスクの撲滅に直結するわけではないといえる。

なお、PCI-DSS 関連規格の策定をおこなっている PCI Security Standards Council では、増加するモバイル端末での電子決済を受け、2012 年 5 月にモバイル決済における留意点をガイドラインとしてまとめている[50]。

(2) 自主規制および業界ガイドライン制定活動

① Do Not Track ヘッダなどウェブトラッキング遮断の仕組み

最近 1～2 年間に米国で特に大きく取り扱われているプライバシー問題として、ウェブサイト運営者が、消費者のウェブ上における行動を追跡する（トラッキング）ことの是非があげられる。この仕組みは、主に自社ウェブサイト・サービス上の広告枠を広告主に販売する事業者により採用されているもので、代表的なものとしては、Google 社の「Google Analytics」や Facebook 社の「Facebook Connect」といったサービスがあげられる。このようなトラッキングの仕組みは、ユーザー行動傾向の詳細な分析を可能とし、高度なパーソナライズサービスやターゲット広告の実現といったメリットをもたらす一方で、行動傾向情報が漏えいした場合の危険性や、「押し付けがましい」広告に対する消費者の嫌悪感、といった短所も指摘されている。

この Do Not Track 機能は、2012 年 2 月に草案が発表された消費者プライバシー権利章典の中で、消費者による自己の情報のコントロールを及ぼすべき事例として明示的に規定されており、今後、民間レベルでの自主規制ガイドラインという形を含め、採用が強化されていくものと考えられる。

民間での取り組みとしては、ウェブ標準推進団体である WWW コンソーシアム（World Wide Web Consortium、W3C）によって、「Do Not Track ヘッダ」と呼称される仕組みの策定が進められている[51]。これは、消費者がウェブブラウザの設定を介し、ウェブサイトに対してトラッキングを行わないよう通知できるようにするもので、主要なブラウザ

[50] https://www.pcisecuritystandards.org/documents/accepting_mobile_payments_with_a_smartphone_or_tablet.pdf

[51] http://www.w3.org/2011/tracking-protection/

の間では、既に Microsoft Internet Explorer、Mozilla Firefox、Apple Safari、Opera が対応している。今やシェア第1位[52]となった Google Chrome は、ブラウザ各社が Do Not Track 対応を進めていた 2011 年 3 月ごろ、外部からの Cookie を遮断するブラウザ拡張機能を Chrome に実装し、トラッキングの可否をウェブサイト事業者の判断に委ねる Do Not Track ヘッダの通知を行う仕組みとは、一線を画していた。しかし、2012 年 2 月の消費者プライバシー権利章典にも Do Not Track への対応が明記されたことから、Google 社も方針を転換し、2012 年内には Do Not Track 対応となる予定である[53]。

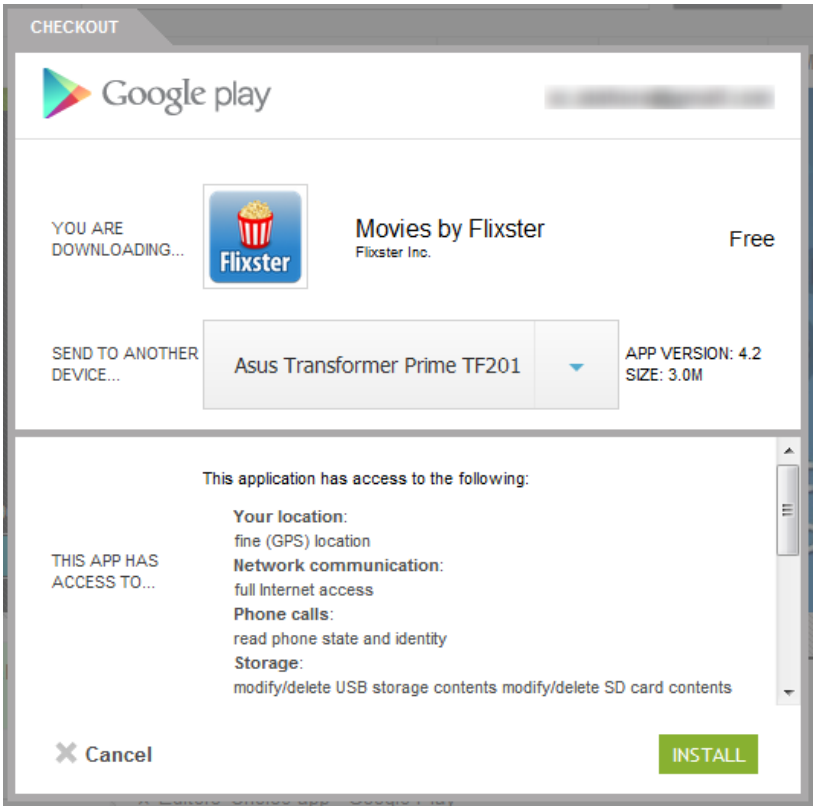
② 収集対象情報の明記

また、近年ではインターネットサービスの提供手段として、Facebook、Twitter、Google+や LinkedIn などソーシャルメディア・プラットフォームや、iOS や Android などモバイル OS 上で稼働するアプリケーションが活用されるようになってきているが、アプリケーションの適切な動作を保証するために、プラットフォームや OS 内に保存されている機微情報に対してアプリケーションがアクセスを求める場合がある。

現在、アプリケーションがプラットフォームや OS 内に保存されているどのような情報にアクセスするかについての情報開示は義務付けられていないものの、各プラットフォーム運営者とも、概ねユーザーに対してこのような情報開示を進めていく方向である。例えば、Google 社運営の Android 向けアプリケーションストア「Google Play Store」では、アプリケーションインストール前に以下のような画面が表示され、アプリケーションがアクセスできる Android 端末上の情報の種類が明確に分かる仕組みとなっている。

[52] http://gs.statcounter.com/#browser-ww-monthly-200807-201206
[53] http://www.computerworld.com/s/article/9224543/Google_commits_Chrome_to_support_Do_Not_Track_

【図表 11：Android アプリケーションインストール前画面[54]】



これに対し、FTC は、オンライン上の情報開示・収集については、ワークショップの開催[55]を行うなど積極的な取組みを行ってきている。アプリケーションによる個人情報収集についても、収集理由が十分に公開されていないとして、FTC は各プラットフォーム運営事業者に対し、更なる情報開示を求める姿勢を強めている[56]。

54
https://play.google.com/store/apps/details?id=net.flixster.android&feature=related_apps#?t=W251bGwsMSwxLDEwOSwibmV0LmZsaXhzdGVyLmFuZHJvaWQiXQ..

55 http://www.ftc.gov/bcp/workshops/inshort/index.shtml

56子供向けモバイルアプリケーションに関する調査結果に基づくもの。
http://www.minonline.com/news/FTC-Slaps-Apps-For-Lax-Privacy-Disclosures_19954.html
http://www.ftc.gov/opa/2012/02/mobileapps_kids.shtm

4. 連邦政府による個人情報・プライバシー保護の取り組み

本章では、連邦レベルでの個人情報・プライバシー保護関連法、消費者保護を担当する連邦取引委員会（FTC）の動向、その他関連する動向について解説する。

(1) 個人情報・プライバシー保護関連法

米国では、個人情報・プライバシー保護に関する規制は、基本的は各州政府や地方政府に委ねられており、連邦政府レベルでは、特定のスコープ、政策目的に限定されている。本項では、これらの連邦法について紹介する。

① HIPAA（Health Insurance Portability and Accountability Act）

1996 年、Bill Clinton 政権時代に成立した Health Insurance Portability and Accountability Act（HIPAA）は、医療保険の対象カバレッジや医療情報の取り扱い、電子化などについて幅広く規定する法律であり、その一環として患者のプライバシーを保護する規定も含まれている。

HIPAA プライバシー条項が対象とする情報（保護医療情報（Protected Health Information, PHI））としては、消費者（患者）の診察・医療記録はもちろんのこと、病歴、医療サービスに対する支払い履歴、生体サンプルなどもあり、これらを取り扱う個人、組織、団体、企業（医師、病院、保険会社、請求処理会社など）に対して HIPAA が定める情報取り扱いルールの遵守が求められている。

HIPAA プライバシー要項の最も基本的な理念は、病院など HIPAA 対象組織が、治療行為や治療費請求、といった医療サービス以外の目的で、患者情報を利用したり第 3 者と共有することを一切禁じる、というものである。加えて、HIPAA では、①患者が自らの情報を閲覧する権利、②患者情報が第 3 者と共有された場合、患者がこの事実を知る権利、の 2 点も規定されており、対象組織が HIPAA に準拠する上で完了すべきプロセスも示されている[57]。

② HITECH（Health Information Technology for Economic and Clinical Health）Act

2009 年に成立した米国再生・再投資法（American Recovery and Reinvestment Act、ARRA）の一部として成立した Health Information Technology for Economic and Clinical Health（HITECH）Act では、HIPAA 遵守義務がある医療機関・保険者などの組織に対して、情報通信の機密性に関する追加要項が課せられている。中でも、特に個人情報・プライバシー保護との関連性が高い要項として、同法は保護医療情報

[57] http://www.stanford.edu/dept/legal/powerpoint/HIPAA-BRIEF-SUMMARY.doc

（PHI）が漏えいした場合には対象者全員への通報を義務付けるとともに、うち 500 人分以上の PHI の漏えいした場合に、健康福祉省（Department of Health and Human Services、HHS）及びメディアに対して通報を行うよう義務付けている、という点がある。更に、同法は HIPAA の適用対象範囲について、「組合（business associates）」を新たに追加している[58]。

HIPAA 及び HITECH 法の遵守状況について、健康福祉省（HHS）ではこれまで監査や是正命令・提訴を行なっている。具体例としては、2009 年にテネシー州の保険者 Blue Cross Shield が PHI57 件を盗難されたことに対する個人情報保護体制の不備を理由として 150 万ドルの罰金及び再発防止対策の整備で合意した件[59]や、2011 年に保険者 Cignet が患者からの情報開示請求を不当に拒否したことなどに対して罰金 430 万ドルを命令した件[60]があげられる。

③ COPPA（Children's Online Privacy Protection Act）

1998 年、Bill Clinton 政権時代に成立した Children's Online Privacy Protection Act（COPPA）は、13 歳未満の子供に関する個人情報のオンラインでの収集について規定する法律である。具体的には、子供の個人情報を収集することを想定する事業者や個人に対して、以下を規定する内容となっている[61]。

- プライバシーポリシに含まれるべき要項
- 子供の保護者から、いつ、どのようにして子供の個人情報収集許可を得るか
- 子供の個人情報保護において、事業者はどのような責任を負うか
- 子供に対するマーケティング、宣伝活動についての制限

このように、十分な自己判断能力を持たないと考えられる子供の個人情報収集について制限する同法であるが、同法に準拠するためには多くの事務処理が必要となることもあり、そのような手間を省くため、または過失的に同法に違反することを防ぐため、Google 社のように 13 歳未満の子供にはサービスを一切提供しないオンライン事業者も見られる[62]。

なお、成立から 10 年以上が経過している同法については、SNS などかつては想定されていなかったサービスが存在する現状にそぐわないとする意見も多く[63]、FTC は

[58] http://www.gpo.gov/fdsys/pkg/USCODE-2009-title42/html/USCODE-2009-title42-chap156-subchapIII-partA-sec17931.htm
http://www.natlawreview.com/article/hipaahitech-enforcement-action-alert
[59] http://www.natlawreview.com/article/hipaahitech-enforcement-action-alert
[60] http://www.hhs.gov/news/press/2011pres/02/20110222a.html
[61] http://www.ftc.gov/ogc/coppa1.htm
[62] http://sunpig.com/martin/archives/2011/07/03/google-made-my-son-cry.html
[63] http://www.law.northwestern.edu/journals/njlsp/v5/n2/7/

2011 年末、COPPA の改革を求めていく姿勢を示している。具体的には、「個人情報」の定義を子供が利用する端末上のデータ（位置情報、写真、動画、IP アドレスなど）にも拡大すること、更に「収集行為」の定義を拡大することも目指されている。加えて、経年データの削除を義務付ける要項や、保護者からの許可取得方法の拡大も想定されており[64]、今後 COPPA の改革に向けた議論が本格化すると考えられる。

④ IRTPA（Intelligence Reform and Terrorism Prevention Act）

2004 年、George W Bush 政権時代に成立した Intelligence Reform and Terrorism Prevention Act（IRTPA）によって、国家情報長官（Director of National Intelligence、DNI）職、国家テロ対策センタ（National Conterterrorism Center、NCTC）、プライバシーおよび市民権監督委員会（Privacy and Civil Liberties Oversight Board、PCLOB）という 3 つのポスト・連邦政府組織が新設されている。

IRTPA 自体は、DNI や NCTC の設立により米国の対テロ体制を強化することを目的としており、その一環として PCLOB に対しては、対テロを名目とした連邦政府の行動が米国市民権を侵害していないかどうか監視する役割が課せられている[65]。しかし、委員ポストには 2008 年から 2011 年 12 月まで空席が存在するなど[66]、DNI や NCTC とは対照的にほとんど具体化されてこなかった。オバマ大統領は、2011 年 12 月にようやく全委員（5 名）の推挙を完了しており、現在は議会による推挙の承認が待たれる状況となっている。

(2) 連邦取引委員会（FTC）の動向

消費者保護を担う連邦取引委員会 Fair Trade Commission (FTC)は、個人情報・プライバシー保護に向けて積極的に動いており、具体的に最近では、以下のような調査、命令発出などを実施している。

【図表 12：FTC による最近の活動事例】

対象	時期	概要
US Search 社	2010 年	個人情報ブローカー事業者の US Search 社が、個人情報の削除について削除申請者から課金していたにも関わらず、その削除方法が不十分であったことを問題視した FTC は、同社を調査。調査の結果、US Search 社の行為は違法であったとして、FTC は虚偽的広告の停止、削除サービスを利用した消費者に対する返金、サービス利用上制約の明記、を命令[67]。

[64] http://www.natlawreview.com/article/ftc-will-propose-broader-children-s-online-privacy-safeguards
[65] http://articles.latimes.com/2010/apr/19/opinion/la-ed-privacy-20100420
[66] http://articles.latimes.com/2010/apr/19/opinion/la-ed-privacy-20100420
http://www.theverge.com/2011/12/22/2651627/obama-privacy-civil-liberties-oversight-board-nominations
[67] http://www.dailyfinance.com/2011/03/28/ftc-says-us-searchs-privacylock-service-did-little-to-block-s/

Rite Aide 社	2010 年	全米第三位の薬局である同社が、薬品ラベルや求職票などをそのままゴミ箱に廃棄するなど、Health Insurance Portability and Accountability Act などが求める個人情報保護体制を取っていなかったとして、FTC と同社は、今後 20 年間、2 年ごとに独立機関による監査を受けることで合意。また、同社は HHS とも百万ドルの制裁金支払いと 3 年ごとに独立機関によるレビューを受けることで合意[68]。
Chitika 社	2011 年	ターゲット広告表示技術を開発する Chitika 社が、同社によるトラッキング行為から明示的にオプトアウトした消費者の意思に反して、消費者を継続的にトラッキングしていたことが表面化し、FTC は同社の調査を開始。結果、Chitika 社の行為は違法であったとして、FTC は虚偽的なオプトアウトの仕組みの停止、オプトアウト方法の明確化などを命令[69]。
Facebook 社	2011 年	Facebook 社が、ユーザーの許可無くユーザー情報を第 3 者（広告主など）と共有していたことを問題視した FTC は、同社の調査を開始。Facebook 社と FTC は、第 3 者とのユーザー情報共有前に明確な形でユーザーの承諾を得ること、今後 20 年間、2 年毎に独立機関による監査を受ける条件で合意[70]。
Google 社	2012 年	Google 社が、Apple 社製ウェブブラウザ「Safari」ユーザーのプライバシー設定を迂回し、設定に関係なく Safari ユーザーをトラッキングできる仕組みを開発、展開していたとして、FTC は同社の調査を開始。調査結果は未発表も、FTC は同社の行為を違法と判断し、約 1,000 万ドルの罰金を課すとの見方が優勢[71]。

また、FTC は、消費者の個人情報・プライバシー保護に向けた報告書やガイドライン類も作成しており、最近発表された代表的な文書には以下のようなものがある。

【図表 13：FTC による最近の報告書・ガイドライン】

タイトル	時期	概要
Self-Regulatory Principles For Online Behavioral Advertising	2009 年	FTC が、オンラインターゲット広告について初めて発行した 2007 年のガイドライン[72]に対するパブリックコメントを考慮し、同ガイドラインをアップデートしたもの。ターゲット広告がもたらすメリットを認めながらも、ターゲット広告に伴うユーザートラッキング行為に関する透明性の欠如に懸念を示す[73]。
Protecting	2010 年	各種消費者向けサービスにおける消費者プライバシー保護を目

68 http://online.wsj.com/article/SB10001424052748703292704575393433473086958.html?_nocache=1339131548691&user=welcome&mg=id-wsj
なお、HIPAA に関する直接的な法執行権限は HHS にあり、FTC はそれを補完する位置づけであることに注意。
69 http://www.ftc.gov/opa/2011/03/chitika.shtm
70 https://www.nytimes.com/2011/11/30/technology/facebook-agrees-to-ftc-settlement-on-privacy.html
71 http://www.theverge.com/2012/5/4/2999451/google-ftc-fine-safari-cookie-tracking
72 http://www.ftc.gov/os/2007/12/P859900stmt.pdf
73 http://www.ftc.gov/opa/2009/02/behavad.shtm
http://www.ftc.gov/os/2009/02/P085400behavadreport.pdf

Consumer Privacy in an Era of Rapid Change: A Proposed Framework for Businesses and Policymakers		的とした枠組みを、一般企業および政策立案者に対して提案する文書。①Privacy by Design（製品・サービスの開発段階からプライバシーに配慮した仕組みを取り込むこと）、②Simplified Choice（消費者の個人情報収集行為について、消費者に明確な選択肢を提供すること）、③Greater Transparency（消費者の個人情報収集行為について、情報開示に努めること）、の 3 点からなる枠組みを提唱[74]。
Final Commission Report on Protecting Consumer Privacy	2012 年	上記の枠組み提唱に対するパブリックコメントを考慮し、最終化したもの。FTC は、上記の枠組み提唱後も業界による自主規制は一部の例外を除き進んでいないと批判した上で、消費者の個人情報を収集する一般企業に対し、FTC の提唱するプライバシー保護に向けたベストプラクティスの早急な導入を要求。また、特にデータブローカー事業者を規制する法案の作成を支援する意向も表明[75]。
Mobile Apps for Kids: Current Privacy Disclosures Are Disappointing	2012 年	子供向けモバイルアプリケーションによる個人情報収集行為についての調査報告書。Apple 社、Google 社が運営するモバイルアプリケーションストアをそれぞれ調査した結果、収集される情報の種類、収集された情報の利活用用途および共有先、などについての情報開示が不足しているとの懸念を表明[76]。

[74] http://www.ftc.gov/os/2010/12/101201privacyreport.pdf
http://www.ftc.gov/opa/2010/12/privacyreport.shtm
[75] http://www.ftc.gov/opa/2012/03/privacyframework.shtm
http://ftc.gov/os/2012/03/120326privacyreport.pdf
[76] http://www.ftc.gov/os/2012/02/120216mobile_apps_kids.pdf
http://www.ftc.gov/opa/2012/02/mobileapps_kids.shtm
http://www.zdnet.com/blog/btl/ftc-voices-concerns-about-mobile-apps-for-children/69638

5. 今後の方向性

本章では、米国における個人情報・プライバシー保護の取り組みについて、今後の方向性を考察する。

(1) 連邦取引委員会（FTC）の活動強化

これまでの連邦政府による取り組みを見ると、基本的には法規制の強化よりは、業界ステークホルダーによる自主規制やガイドライン策定を促進することに重点が置かれていたと考えられる。

実際に、2012 年 3 月に FTC によって発表された「Final Commission Report on Protecting Consumer Privacy」では、原則として、今後も FTC が掲げる 3 点の枠組みに沿った業界自主規制の強化を促進する方針が表明されており、上記文書中で、FTC は Do Not Track 条項を「業界による自主規制の成果」として取り上げており[77]、民間による取り組みに一定の評価を与えていることは事実といえる。

しかし、今般、FTC は民間による自主規制の取り組みについて批判的な意見を示しており、より早急に自主規制に取り組むことを業界ステークホルダーに求めると同時に、2012 年 2 月に発表された「消費者プライバシー権利章典」を受け、議会における個人情報・プライバシー保護に向けた立法活動の支援を行うことも表明している。同権利章典では、「産学官連携による、法的拘束力のある行動規範の策定」が今後の方針の 1 つとして取り上げられているように、2012 年以降の米国では、民間による自主規制のみに依存しない方向性も模索されるものと考えられる。

また、今後も米国と EU 間で事業者が情報交換を円滑に行えるよう、既存の US-EU セーフハーバー規定を活用していく方向が示されている（上述）。このセーフハーバー規定は、商務省への自己申告が基本ではあるものの、EU 指令（今後は規則）への遵守状況の確認については、FTC も不公正な取引の禁止の観点から監督権限を有しており、今後、グローバルな個人情報保護ビジネスが拡大していく中で、FTC の活動範囲も広くなってくることが想定される。

(2) 「忘れられる権利（right to be forgotten）」を巡る議論

EU では現在、自己に関する情報コントロール権の一環として、「忘れられる権利（right to be forgotten）」と称される権利を保障するための議論が展開されている。忘れられる権利とは、Do Not Track 要項のようなオンラインでの消費者行動のトラッキングを拒否

[77] http://ftc.gov/os/2012/03/120326privacyreport.pdf

する権利に留まらず、消費者が各種サービスプロバイダに対して個人情報の削除も求められる権利も包含する概念である[78]。

このような権利の保障は消費者プライバシー保護の強化に寄与するといえるものの、その具現化に向けては、技術的な問題（電子情報の複製阻止が困難である点など）のみならず、言論の自由との兼ね合いといった政治的・文化的な問題も予想されている。例えば、2012 年 3 月には、東京在住の男性が、Google 社ウェブ検索サービスにおいて自身と関係のない犯罪行為が自身の名前と関連付けられて「サジェスト」されることを懸念し、このような「サジェスト」の削除を Google 社に求めた事実が報道されている[79]。このような要求に対して、Google 社は 2012 年 5 月、ウェブ検索エンジンは言論の自由に基づく保護対象の範疇に入ると主張する文書を発表しており[80]、原則として検索結果や「サジェスト」結果の削除には一切応じない姿勢を見せている。

また、現在ほとんどのウェブ・モバイルアプリケーション事業者は、ユーザーに対して無料でアプリケーションを提供する一方、アプリケーションに表示される広告からの収入に頼っているという現状がある。その中で、仮に「忘れられる権利」といった、一般企業による個人情報収集・保有を大幅に制限する権利が保障されると、事業者としてはターゲット広告のような収入源が絶たれることになり、ひいてはインターネット技術革新の衰退につながる、とする意見も見られる[81]。

個人情報・プライバシーの保護強化に関する動向は、現在米国で幅広い関心を集めており、今後は官民両面から規制や枠組み策定が進むと考えられる。しかし、その実現化に向けた課題も多く、今後更に慎重な議論が重ねられるものと見込まれる。

なお、このレポートに対するご質問、ご意見、ご要望がありましたら、
takashi_wada@jetro.go.jp までお願いします。

[78] http://ec.europa.eu/justice/data-protection/document/review2012/com_2012_11_en.pdf
[79] http://news.yahoo.com/man-wins-injunction-against-google-claiming-auto-complete-125806868.html
[80] http://paidcontent.org/2012/05/09/search-engines-have-same-speech-rights-as-new-york-times-says-google-report/
[81] http://www.computerworld.com/s/article/9223717/Critics_EU_s_proposed_data_protection_rules_could_hinder_Internet