米国における個人情報保護に関する取り組みの現状

八山　幸司
JETRO/IPA New York

1　はじめに

多様な IT サービスが急速に普及している米国では、様々な電子データを活用しようとする企業や政府と個人情報保護を懸念する国民との間で、個人情報保護に関する議論が高まっている。米国では特に近年、政府の通信傍受の暴露や、繰り返し発生する情報漏えい事件、なりすまし犯罪の増加など、個人情報保護の脅威となる出来事が数多く発生した。一方で、ビッグデータや IoT（Internet of Things／モノのインターネット）[1]などデータを活用した技術は人々の生活の中に浸透してきており、今後ますますデータを活用したビジネスが活発になるものと考えられる。将来、ビッグデータや IoT を活用したビジネスが成長産業に育っていくためには、データベースに蓄積された個人情報がどのように扱われるかについて、人々の懸念をいかに払拭できるかが重要である。人々が電子データとしての個人情報にどのような決定権を持つことができるかの模索も続いている。今号では、急速に発展する IT サービスやテクノロジーに対応した次世代の個人情報個人情報保護について、政府、企業、社会で議論が続く米国の個人情報保護について紹介する。

最初に、米国における個人情報保護に関する動向を紹介する。米国の情報漏えい事件は増加する一方で、発生件数では公的機関に届け出のあったものだけでも世界全体の情報漏えい事件の 72%を占めるほどとなっており、近年では医療分野を標的とした案件が急増している。また、個人情報を悪用する、なりすまし犯罪も未成年者への被害が大きい。近年発生したサイバー攻撃による情報漏えいでは、米連邦人事管理局（Office of Personnel Management）、ソニー・ピクチャーズ・エンタテインメント社、アシュレイ・マディソン事件などがある。

次に企業の動向について紹介する。データの活用が中心となる IoT とビッグデータは特に個人情報保護が重要となるため、専門家はこの 2 つのテクノロジーに対する個人情報の取り扱いについて提言を出している。しかしながら、IoT デバイスのセキュリティ面への懸念は後を絶たず、スマートホームやドローン等に用いる IoT デバイスの脆弱性がセキュリティ企業から指摘される事態が発生している。スマートフォンメーカーは消費者の個人情報の流出への懸念を払拭するために、スマートフォン端末のデータの暗号化や様々なセキュリティ機能を搭載してきている。またソーシャル・ネットワーキング・サービスを提供する Facebook 社では、ユーザーのデータを活用した広告戦略を展開させており、個人の行動を追跡することが可能なターゲット広告の技術を作り出しているが、プライバシーに対する懸念も高まっており、同社ではユーザーが広告機能の利用について選択できるようにしている。

米国における個人情報保護に関する法律は、テクノロジーの発達とともに、その時代に対応した個人情報保護関連の法律が分野別に作られてきた。オバマ政権はビッグデータの推進や消費者のプライバシー権利の確立の中で個人情報保護を打ち出してきたが、近年発生した情報漏えい事件や政府による通信傍受の暴露を受けて、新しい個人情報保護政策を打ち出してきている。また、州政府も各州で声が上がっている問題に取り組むために独自の個人情報保護に関する法を成立させている。

最後に個人情報保護に関連した最先端技術を紹介する。スイスのスマートフォンメーカーSilent Circle 社が開発する BlackPhone 2 は、1 台のスマートフォンの中に、データが共有されない複数の OS の利用環境を作りだすことができることから、1 台で会社用とプライベート用に使い分けることも可能となっている。教育プ

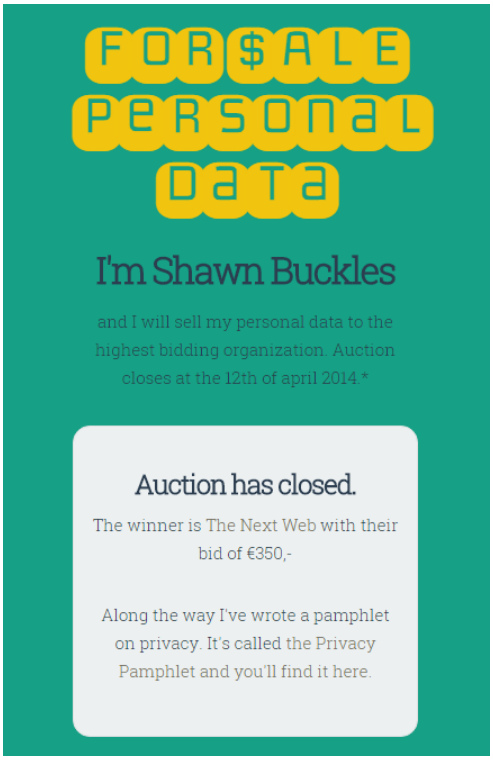
[1] 様々なデバイスをインターネットへ接続させる構想。デバイスから様々なデータを収集することで、デバイスやロボット同士の連携や、人々の生活をサポートする情報の分析に役立てることができる。

ラットフォームを提供する Clever 社は、学校が使用する教育アプリがプライバシーポリシーに乗っ取ったデータの取り扱いをしているか監視することが可能である。カリフォルニア大学では、指紋の凹凸まで認識可能な 3D 指紋認証技術の開発に成功している。

インターネット上でのビジネスやコミュニケーションが活発化する一方で、サービスの利用と個人情報保護のバランスについて様々な議論が続けられている。あるオランダの大学生は、自分の住所から医療情報、スケジュールや思想に至るすべての個人情報をオークションに出品し、自分の個人情報に値段をつけた。彼は、人々がインターネット上のサービスを無料で利用するのと引き換えに多くの個人情報を提供していることを認識していないと語り、自ら個人情報に値段をつけることで、インターネット上における個人情報の収集とプライバシーがどのようなものかを見せた[2]。数多くのインターネットビジネスが展開される米国で、政府、企業、社会それぞれによる個人情報保護への取り組みについて紹介する。

図表 1 は個人情報をオークションに出品した Shawn Buckles 氏とオークションのウェブサイトとなっている。

図表 1：Shawn Buckles 氏とオークションのウェブサイト



出典：Shawn Buckles[3]、ABC News[4]

[2] http://www.wired.co.uk/news/archive/2014-04/15/shawn-buckles-is-worth-350-euros
[3] http://shawnbuckles.nl/dataforsale/
[4] http://abcnews.go.com/Technology/dutch-student-shawn-buckles-sold-digital-soul-highest/story?id=23438324

2　個人情報保護に関する事件・動向

（1） 米国における個人情報保護

a. 近年の個人情報の動向

米国における個人情報は、個人識別情報（Personally Identifiable Information）とも呼ばれ、特定の個人を識別する手がかりになる可能性のある様々な情報を指し、その中には名前、生まれた場所や日時、母親の旧姓、生体記録、社会保障番号（Social Security Number）などが含まれる。他にも、単独では個人を特定できなくとも他の情報と組み合わせることで個人の識別が可能な情報として、診療記録、教育、財政状態、雇用などの情報がある[5]。

IC カードベンダーGemalto 社と情報セキュリティ企業 Safenet 社の調査によると、2014 年に発生した情報漏えいは公的機関に届け出のあったものだけでも世界全体で 1,541 件となっており、流出したデータは約 10 億 2,310 万件にのぼったとされている。その中で米国の情報漏えいの発生件数は 1,107 件と全体の約 72%を占めるほどとなっている[6]。米国で近年発生した主な情報漏えい事件として以下のようなものある[7]。

企業名	セクター	流出件数	推定被害額	発生年
Office of Personnel Management（連邦人事管理局）	政府	2,210 万件	1 臆 3,300 万ドル～3 臆 2,980 万ドル	2015
Anthem	保険	8,000 万件	80 億～160 億ドル	2015
Ashley Madison	インターネット	3,300 万件	8 億 5,000 万ドル	2015
eBay	インターネット	1 億,4,500 万件	2 億ドル	2014
JPMorgan Chase	金融	8,300 万件	10 億ドル	2014
Home Depot	小売	5,300 万件	8,000 万ドル	2014
Sony Pictures Entertainment	メディア	3,000 件	3,500 万ドル	2014
Target	小売	7,000 万件	2 億 5,200 万ドル	2013

米調査会社 Ponemon Institute 社によると、米国における被害の 2014 年の年換算コストは 1,270 万ドルに上り、5 年前に比べて 96%の増加となっている。また、事態の収拾にかかる時間もこれまでより 33%長くなっていることが被害額の増加に拍車をかけており、平均被害額は 160 万ドルという結果も出ている[8]。

個人情報の盗難被害を取り扱う非営利組織 Identity Theft Resource Center に届け出のあった情報漏えいをセクター別に見ると、2008 年から 2011 年にかけては企業による情報漏えいが最も多かったものの、2014 年は医療分野の情報漏えいが 42.5%と突出していた[9]。医療分野における情報漏えいが急増した背景には、医療機関データベースのセキュリティ対策が遅れていることや、ブラックマーケットで医療情報がクレジットカード番号などのおよそ 10～20 倍の価格で取引されていることから、営利目的での情報の盗難が

[5] https://ico.org.uk/for-organisations/guide-to-data-protection/key-definitions/
[6] http://breachlevelindex.com/pdf/Breach-Level-Index-Annual-Report-2014.pdf
[7] http://www.bankrate.com/finance/banking/us-data-breaches-9.aspx
http://www.reuters.com/article/2015/07/09/us-cybersecurity-usa-idUSKCN0PJ2M420150709
http://www.engadget.com/2015/09/02/opm-data-breach-identity-theft-protection/
[8] http://www8.hp.com/us/en/hp-news/press-release.html?id=1815969#.VfMhDxFViko
http://business.financialpost.com/fp-tech-desk/hack-attacks-hit-home-the-kind-of-thing-that-ceos-get-fired-for?__lsa=d87c-1885
[9] http://www.idtheftcenter.org/ITRC-Surveys-Studies/2008-data-breaches.html

増えている[10]。米国のある保険会社のサイバー保険の担当者に話を聞いた際も、医療関連の個人情報が最も機微に感じるとのことであり、同分野における個人情報保護の対策強化が必要と考えられる。

図表 2 は、各分野における個人情報漏えい事件の発生比率を示したものとなっている。

図表 2:各業界における個人情報漏えい事件の発生比率

業界	2005		2008		2011		2014	
ビジネス	25	15.9%	237	**36.1%**	177	**42.0%**	258	33.0%
教育	75	**47.8%**	131	20.0%	57	13.5%	57	7.3%
政府・軍事	21	13.4%	110	16.8%	54	12.8%	92	11.7%
医療関係	16	10.2%	99	15.1%	102	24.2%	333	**42.5%**
金融・	20	12.7%	79	12.0%	31	7.4%	43	5.5%
	157		656		421		783	

出典:Identity Theft Resource Center のデータを元に作成[11]

b. なりすまし

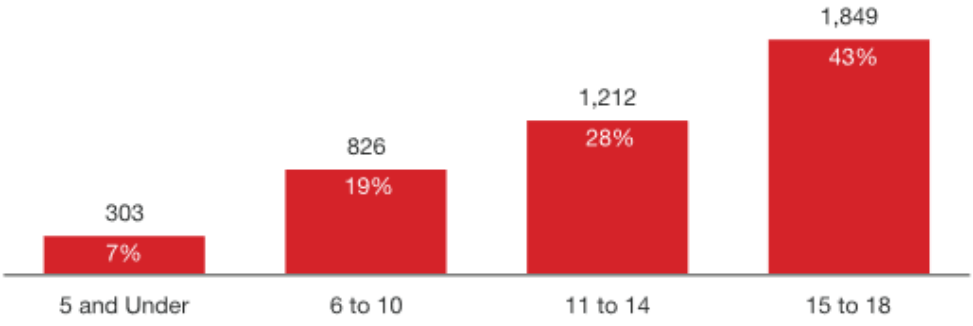
米国の個人情報に関する犯罪の傾向として、未成年の個人情報を悪用した犯罪の増加がある。米国では国民に社会保障番号(Social Security Number)と呼ばれる 9 桁の番号が割り当てられ、納税や社会保障を受ける際に使用されている。この社会保障番号は個人ごとに異なるため、クレジットカードの申請や銀行口座の開設など個人識別が必要なサービスでも利用されることが多く、犯罪歴や信用情報にも使用されている[12]。そのため、社会保障番号を不正に利用した、なりすまし犯罪が後を絶たない。特に近年多いのが、未成年の社会保障番号を悪用した犯罪である[13]。

未成年の社会保障番号は信用情報や犯罪歴がないため、一般的にクレジットカードの承認が下りやすい。本人が 18 歳になってクレジットカードを申請する際に初めて信用情報を確認することになるため、なりすましが発覚するまでに時間がかかるなど悪用しやすいことから、なりすましの標的となるわけである。Carnegie Mellon University のサイバーセキュリティの研究所 CyLab が、2011 年に 4 万人の未成年者を対象に調査したレポートによると、米国の未成年者の 10.2%がなんらかの形で他者に社会保障番号を不正利用されていたことがわかっている。大人が社会保障番号を悪用されたケースはわずか 0.2%であり、未成年者の被害は大人の 51 倍にも達する。また、なりすまし犯罪の被害者となった 4,311 人の未成年者のうち、303 人が 5 歳未満であり、最年少はわずか 5 か月の乳児であった[14]。

図表 3 は、なりすまし犯罪で被害を受けた未成年者の数と年齢層となっている。

[10] http://www.reuters.com/article/2014/09/24/us-cybersecurity-hospitals-idUSKCN0HJ21I20140924
[11] http://www.idtheftcenter.org/ITRC-Surveys-Studies/2008-data-breaches.html
[12] https://www.privacyrights.org/fs/fs10-ssn.htm
[13] http://www.usatoday.com/story/money/personalfinance/2015/09/11/children-victims-identity-theft/72091926/
[14] https://www.cylab.cmu.edu/files/pdfs/reports/2011/child-identity-theft.pdf

図表 3:なりすまし犯罪で被害を受けた未成年者の年齢分布



AGE DISTRIBUTION	ACTUAL	PERCENTAGE
5 and Under	303	7%
6 to 10	826	19%
11 to 14	1,212	28%
15 to 18	1,849	43%

出典:Carnegie Mellon University, CyLab[15]

なお、米国でも子供の段階から納税やクレジットカードの手続きをすることはないものの、親が税金の確定申告のために子供の社会保障番号を取得するため、子供はなんらかの形で社会保障番号を取得することとなる。個人の信用情報を管理している企業は 18 歳以下については信用情報を作成しないようにしている。しかしながら、社会保障番号に登録している名前や年齢を社会保障庁(Social Security Administration)に確認しないため、他社から信用情報を受け取る際に実際に誰かが社会保障番号を確認せずに情報を受け取ることとなり、受け取った信用情報がそのまま履歴として残ってしまうのが現状となっている[16]。

(2) サイバー攻撃による情報流出

a. 米連邦人事管理局の個人情報流出事件

米連邦政府は数多くのサイバー攻撃にさらされており、昨年だけでも 6 万 1 千件もの攻撃が確認されている[17]。2015 年 4 月及び 6 月に起こった連邦政府職員の個人情報流出事件は、その規模において最大級であるだけでなく、諜報機関及び軍関係者が採用される際に行われる機密取扱者の人物調査内容もハッキングされた可能性が指摘されている。

4 月に発覚したのは、420 万人の現職員及び元職員の個人情報への不正アクセスであった。4 月の事件の調査が進む中、引き続き 6 月に新たに現職員、元職員、または職員候補者の人物調査情報を含む個人情報への不正アクセスが明るみになった。それには 2150 万人の社会保障番号なども含まれていたとされている[18]。この事件を受けて、米政府は身元が犯人によって悪用された場合、第三者の民間企業と協力して、

[15] https://www.cylab.cmu.edu/files/pdfs/reports/2011/child-identity-theft.pdf
[16] http://www.usatoday.com/story/money/personalfinance/2015/09/11/children-victims-identity-theft/72091926/
[17] http://www.businessinsider.com/5-facts-that-explain-cyber-warfare-2015-6
[18] https://www.opm.gov/cybersecurity/
http://www.washingtonpost.com/news/powerpost/wp/2015/08/24/opm-hit-in-one-sustained-attack-lessig-exploring-white-house-run-more-ashley-madison-data-coming/
http://www.businessinsider.com/level-of-damage-omp-hack-2015-6

向こう 3 年間無償で被害者をサポートするなどの対応策を発表している[19]。2015 年 7 月には、職員の人事情報を管理する米連邦人事管理局（Office of Personnel Management：OPM）の長官 Katherine Archuleta 氏が、情報流出の責任を取って辞任した[20]。

図表 4 の左は米連邦人事管理局となっており、右は議会で説明を求められる Katherine Archuleta 氏となっている。

図表 4：米連邦人事管理局（左）と Katherine Archuleta 氏（右）

出典：Engadget[21]、The Washington Times[22]

これらの情報が悪意あるハッカーの手に渡った場合の危険は計り知れないため、米国家情報長官はサイバー攻撃を、テロリズム、諜報活動、大量破壊兵器よりも重要な最優先事項に挙げている。現時点ではまだ国家を揺るがすような事件は起こっていないが、例えば「諜報機関及び軍関係者が採用される際に行われる機密取扱者の人物調査の内容」などが悪用されれば、そのような任務に就く人材やその家族に危険が及ぶ可能性もあり、ひいては国家そのものの脅威となりうるからである[23]。

b. ソニー・ピクチャーズ・エンタテインメント社へのハッキング事件

2014 年 10 月に起こった Sony Pictures Entertainment(SPE)社へのハッキング事件では、従業員の個人情報のほか、未公開の映画関連情報など 25 ギガバイト以上のデータへ不正アクセスがあった。被害を受けた従業員数は 6,000 人以上に上り、本名、従業員番号、社会保障番号、ネットワークのユーザー名、基本給、誕生日を含む個人情報が盗難にあった。犯人は自らを「Guardians of Peace（平和の守護者）」と名乗り、同社が配給元となっていた映画の公開を中止しなければ、オンライン上で不正入手した情報を公開するという脅迫文や、犯人の言うことを聞かなければ、従業員やその家族を殺害するなどと数回に及ぶ脅迫を行った。脅迫の中で公開中止を要請されていた映画が、北朝鮮の政治風刺がテーマだったことから、複数のメディアによって北朝鮮政府がハッキングに関与したとの報道があったが、その後ハッキングされた内容をなんらかのルートで手に入れた各メディアが次々とその内容を報道したことから、メディアの倫理を問う問題にも発展した。

図表 5 は、Sony Pictures Entertainment 社のスタジオとなっている。

[19] https://www.opm.gov/news/releases/2015/07/opm-announces-steps-to-protect-federal-workers-and-others-from-cyber-threats/
[20] http://www.cnn.com/2015/07/10/politics/opm-director-resigns-katherine-archuleta/
[21] http://www.engadget.com/2015/09/02/opm-data-breach-identity-theft-protection/
[22] http://www.washingtontimes.com/news/2015/jun/17/obama-still-backs-opm-chief-despite-data-breach/
[23] http://www.businessinsider.com/5-facts-that-explain-cyber-warfare-2015-6

図表 5：Sony Pictures Entertainment 社

出典：Engadget[24]

セキュリティ会社である Alien Vault 社の破壊工作ソフトの専門家によると、このサイバー攻撃の IP アドレスは、ボリビア、キプロス、イタリア、ポーランド、タイを経由して米国というルートをたどっており、調査を行った FBI も、これは非常に高度で手の込んだ攻撃であると言及している。この事件を受けて、SPE 社は被害にあった従業員、または被害にあった可能性のある従業員に事件発覚後 1 週間で連絡を取り始め、個人情報保護サービス提供事業者 AllClear ID 社に依頼する形で、発覚から 1 年間の無料サポートを提供することと確約した[25]。

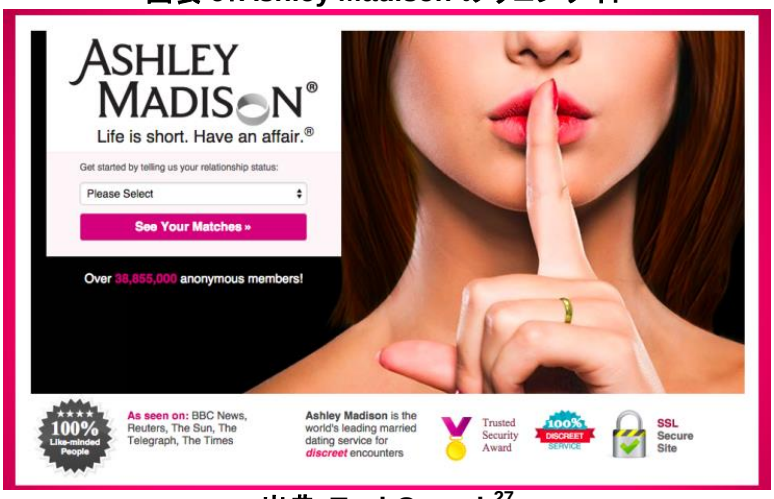
c. アシュレイ・マディソン事件

カナダに本社があり、日本を含む 53 か国に会員がいるとされる不倫専門の出会い系サイト、Ashley Madison についてもハッキングの対象となっている。具体的には、同サイトへの登録者 4,100 万人のうち 3,700 万人[26]の個人情報がハッキングされたことが 2015 年 7 月に判明した。盗難にあったデータの容量は 30 ギガバイトを超えており、自らをインパクト・チーム（The Impact Team）と名乗る犯人は同サイトを運営する投資会社である Avid Life Media 社を相手どり、サイトの運営を直ちに中止しなければ個人情報を公開すると脅迫した。だがサイトの運営は継続され、その後公開された個人情報により、リアリティ番組のスターである Josh Duggar 氏が、実際にサイトの利用者として確認された。さらにホワイトハウス、米国議会、米司法省などで要職に就く人物を含む、数百人に上る公務員が職場の IP アドレスから同サイトにアクセスしていたことなどが判明するなど、事件は大きな問題となった。また登録者として名前が公開されてしまった牧師など数人が自殺を図るという事態に発展したことも、この事件が大きな波紋を呼ぶ要因になっている。

図表 6 は、Ashley Madison のウェブサイトとなっている。

[24] http://www.engadget.com/2014/12/10/sony-pictures-hack-the-whole-story/
[25] https://www.washingtonpost.com/news/the-switch/wp/2014/12/18/the-sony-pictures-hack-explained/
http://www.nytimes.com/2014/12/15/opinion/aaron-sorkin-journalists-shouldnt-help-the-sony-hackers.html?_r=1
http://www.businessinsider.com/sony-pictures-hack-stolen-employee-2014-12
[26] ただし今回のハッキング事件で、同サイトに登録している女性会員の多くが架空の人物だったことがわかっているため、実際の被害者数はこれより少ないと見られている。

図表 6：Ashley Madison のウェブサイト



出典：TechCrunch[27]

その後犯人は、登録者の個人情報に続いて、同サイトのソースコードとモバイルプロパティを公開するという行動にまででており、これにより、他のハッカーがソースコードを分析して、サイトの脆弱な部分からサイバー攻撃をしかける可能性が飛躍的に高まった。Avid Life Media 社はサイバーセキュリティ会社である Cycura 社と連携して、ハッキングの調査と対応にあたっているが、犯人によるソースコードの公開が、同サイトのセキュリティ強化への大きな妨げとなったことは否めない。さらにソースコードには、同社の知的財産に該当する情報が含まれていたため、今秋に予定されていたロンドン株式市場における同社の上場を著しく損ねると見られている。

なお、同社は新規株式公開にあたり、2 億ドルの資金調達を目論んでいたとされる。こうした状況から、同サイトの創設者であり、Avid Life Media 社の CEO を務めていた Noel Biderman 氏はその翌月に辞任するという事態にまで発展している[28]。

[27] http://techcrunch.com/2015/08/24/hackers-now-going-after-ashley-madison-targets/
[28] http://www.wired.com/2015/08/ashley-madison-hack-everything-you-need-to-know-your-questions-explained/
http://www.forbes.com/sites/thomasbrewster/2015/08/28/ashley-madison-ceo-steps-down-after-catastrophic-attack/
http://money.cnn.com/2015/09/08/technology/ashley-madison-suicide/
https://www.ashleymadison.com/

3 企業の動向

（1） IoT とビッグデータにおける個人情報保護

IoT（Internet of Things：モノのインターネット）とビッグデータを活用したデータの分析は、データから生まれる利益と個人のプライバシーのバランスをどのように取るかという点で議論が高まっている。IoT は社会全体から様々な情報を集め、ビッグデータは集められた膨大なデータを使って様々な分析に役立てることができるが、IoT から集められた個人情報がビッグデータによりプライバシー侵害のリスクを高める危険性がある。2014 年 10 月に開催された個人情報保護に関する監視機関や専門家が集まる国際会議、第 36 回データ保護プライバシー・コミッショナー国際会議（36th International Conference of Data Protection and Privacy Commissioners）では、IoT とビッグデータの利用により起こうる個人情報保護侵害のリスクが議論の中心となった。会議では「Internet of Things におけるモーリシャス宣言」が公表され、その中で以下のような内容が提言されている[29]。

- IoT デバイスから集められた情報により構成されるビッグデータは、個人情報として扱われるべきである。
- IoT の価値はデバイスだけでなく、データを使って生み出されるサービスにも価値がある。
- IoT はデータを集めることが前提であるため、消費者が IoT デバイスを購入する際には情報の取扱いについて理解できる形で伝える必要がある。
- データと個人情報の保護は設計段階から考慮されるべきであり、イノベーションの重要なセールスポイントとする。
- データの処理をデバイス内で処理することがセキュリティリスクの低減につながるが、それが難しい場合にはデバイス間の暗号通信を確実にする。
- データと個人情報保護について監督する機関は法整備を進め、違反があった場合には適切な法執行を行う。
- 様々な課題に取り組んでいくために、IoT にかかわるすべての関係者は IoT の導入と派生するビッグデータについて建設的な議論を進める。

また、企業は可能な限りデータを集めて様々な分析に役立てる傾向があるため、個人情報保護を考える上では利用制限にばかり目が行きがちであり、不要なデータを集めないという点が見過ごされがちであるという指摘もある[30]。マサチューセッツ工科大学の研究によれば、個人情報が消されているクレジットカードの利用記録でも、4 回分の記録があれば 90%の確率で個人の特定が可能であり、他の利用記録のデータベースと照らし合わせれば同一人物の追跡が可能とのことである[31]。

個人情報の保護を高めるために不要なデータを取得しない例として、2014 年 10 月からサービスが開始された Apple 社のモバイルウォレットサービス Apple Pay がある。Apple Pay は店頭で携帯電話などを使って電子決済ができるサービスだが、トークン化と呼ばれる手法を使って支払い情報を店舗や Apple 社には渡さず、カード会社に直接送られる仕組みをとっている。支払い情報が必要以上に残されないため、2013 年に発生した米大手小売店 Target 社の POS システムからの情報流出のような事態を防ぐことが可能であり、Apple 社は個人情報保護の高さを Apple Pay のセールスポイントの 1 つに打ち出している[32]。

[29] http://www.bna.com/worlds-data-protection-n17179897174/
http://www.privacyconference2014.org/media/16596/Mauritius-Declaration.pdf
[30] http://www.slate.com/articles/technology/future_tense/2014/11/big_data_underground_railroad_history_says_unfettered_collection_of_data.html
[31] http://gizmodo.com/anonymized-credit-card-data-really-isnt-very-anonymous-1682731883
[32] http://mashable.com/2014/10/23/apple-pay-is-more-secure-than-your-credit-and-debit-cards/#S668jeO4BSkh

とはいえ、IoT デバイスのセキュリティ面そのものへの懸念は後を絶たないのが現状である。2015 年 8 月には、スマートホーム用プラットフォームを販売する ZigBee 社の IoT デバイスの脆弱性がセキュリティ企業 Cognosec 社によって指摘された。ZigBee 社の IoT デバイスは、他の IoT デバイスからの接続を受ける際に認証キーのやり取りを発生させる仕組みとなっているが、そのやり取りが暗号化されていなかったため、ハッカーが認証キーを傍受できるというのである。同社のプラットフォームにはソニー、東芝、Phillips 社、Siemens 社など多くのメーカーが参加しており、プラットフォーム上のすべての IoT デバイスを乗っ取ることができるとまで指摘され、実際の Cognosec 社の実験では Phillips 社のスマート電球へ侵入して脆弱性が証明された。Cognosec 社の研究者は今回のセキュリティ脆弱性の問題点として、IoT デバイスのこのような不具合に対してユーザーが何もできることはなく、影響が大きいにもかかわらずメーカーの対応がいつになるか不透明なままであるということを指摘している[33]。

図表 7 は、スマート電球を使用した際のイメージとなっている。

図表 7:スマート電球の使用イメージ

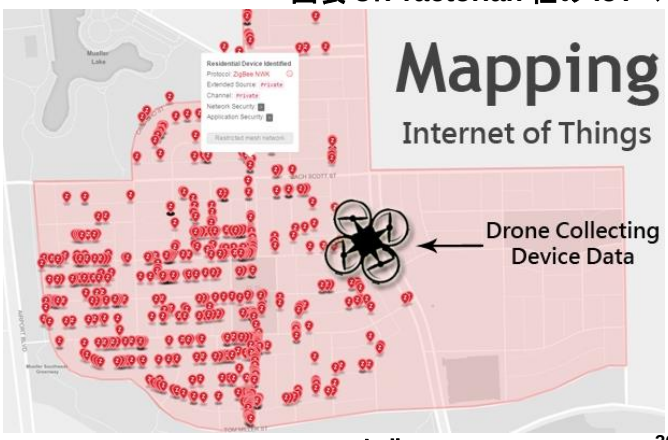
出典:Slash Gear[34]

セキュリティ企業 Praetorian 社についてもドローンを使った IoT マップを作成する実験の過程で、ZigBee 社の脆弱性を見つけ出したことを明らかにした。同社がテキサス州オースティンでドローンを使って IoT デバイスの調査をしていたところ、ZigBee 社の IoT デバイスが暗号化されていない形でネットワークを開いていたことを発見したという。同社の IoT マップでは、ZigBee 社の製品を含む 1,600 の IoT デバイスを発見しており、ドローンを使用することで容易に情報収集が可能であることが指摘されている。2015 年 7 月にセキュリティ企業 Hacking Team 社が、Boeing 社と提携してスパイウェアを送り込むドローンを開発したことが発表されており、ドローンを使ったハッキングは現実のものになろうとしている[35]。

図表 8 の左は Praetorian 社の IoT マップとなっており、右が調査に使用したドローンとなっている。

[33] http://thehackernews.com/2015/08/hacking-internet-of-things-drone.html
http://fortune.com/2015/08/07/zigbee-hacked/
[34] http://www.slashgear.com/philips-hue-ipad-controlled-led-lightbulbs-hands-on-29254444/
[35] http://www.techinsider.io/how-drones-can-hack-your-home-2015-8

図表 8：Praetorian 社の IoT マップ（左）とドローン（右）



出典：The Hacker News[36]、Tech Insider[37]

（2） スマートフォンにおける個人情報保護

スマートフォンの個人ツールとしての利用が広がる中で、普及の大きい iPhone および Android 搭載スマートフォンメーカーはユーザーの個人情報保護のために様々な対応を進めている。これは、いくつかの事件を通してスマートフォンをめぐる個人情報保護の問題が取り沙汰されてきたためである。例えば、2013 年に発生したスノーデン事では米国家安全保障局（National Security Agency：NSA）が携帯電話を含めた通信の傍受をしていたことから、スマートフォン利用におけるプライバシー面の懸念が一気に高まった。特に Apple 社の iPhone では、電源を切っていても NSA が通話の傍受が可能であるとスノーデン氏に公表されたり[38]、以前のバージョン iOS 7 で暗号化通信が行われないというバグが見つかるなどの事態が続いていたといった点も影響している[39]。

このような経緯を経て Apple 社は、暗号化の仕組みを変更し、2014 年 9 月にリリースした iOS 8 から自社で iPhone の暗号キーを所有しないことを表明した。これは、暗号化された端末上のデータを複合するための暗号キーを持たないことで、Apple 社がユーザーの iPhone 内の情報を直接見ることができない仕組みにすることで、警察など第三者機関から依頼されてもデータの引渡しを技術的に不可能にしたというものである[40]。この Apple 社の動向を追随するように、Google 社も 2014 年 11 月にリリースした Android 5.0 で端末上のデータの暗号化する機能を標準搭載するなど、ユーザーの個人情報保護を重視した対策をとっている[41]。

このような両社の個人情報保護策に対し、連邦捜査局（Federal Bureau of Investigation：FBI）の James Comey 長官は個人情報保護の重要性を理解しているとしながらも、テロや誘拐事件などの捜査に必要な情報の取得が難しくなり、法の及ばないところで使用できる製品を売り出そうとしていると非難するなど、個人情報保護と国家安全保障のバランスの難しさを示している[42]。

[36] http://thehackernews.com/2015/08/hacking-internet-of-things-drone.html
[37] http://www.techinsider.io/how-drones-can-hack-your-home-2015-8
[38] http://www.wired.com/2014/06/nsa-bug-iphone/
[39] http://www.wired.com/2014/02/gotofail/
http://fortune.com/2014/02/23/apples-security-bug-five-nsa-conspiracy-theories/
[40] http://gizmodo.com/apple-wont-turn-over-your-phones-data-to-police-if-your-1636197341
[41] http://www.engadget.com/2015/03/02/android-lollipop-automatic-encryption/
2015 年 3 月の Android 5.1 へのアップデートで標準設定をオフにしており、ユーザーが自分で暗号化をオンにする必要がある。
[42] http://www.huffingtonpost.com/2014/09/25/james-comey-apple-encryption_n_5882874.html

なお、iOS と Android の最新バージョンでは、さらに様々なセキュリティ機能が追加されている。Apple 社が 2015 年 9 月にリリースした iOS 9 ではパスワードが 4 桁から 6 桁に変更されており、クラウドサービス iCloud への接続に使われる 2 段階認証[43]と合わせてアカウントの不正利用へのセキュリティを強化している。また、アプリによるインターネットへの通信をすべて暗号化（HTTPS 通信）にする App Transport Security 機能も追加された[44]。Google 社がリリース予定の Android 6.0 では、アプリごとに個人データへのアクセスを許可するか設定できるようになり、指紋認証機能もサポートされることとなった。これらは iPhone で搭載されていたが、Android もセキュリティ機能を強めてきている[45]。

図表 9 の左が iOS 9 となっており、右が Android 6.0 となっている。

図表 9：iOS 9（左）と Android 6.0（右）

出典：Apple、BGR[46]

（3） ソーシャルメディア（Facebook）における個人情報保護

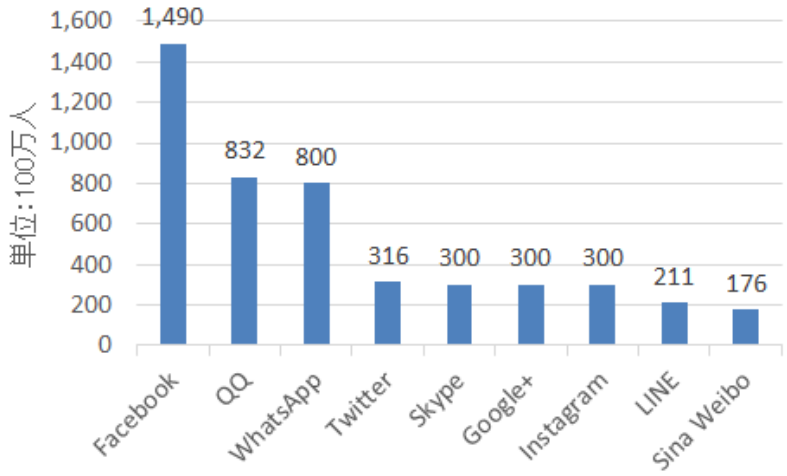
ソーシャル・ネットワーキング・サービス（SNS）大手の Facebook でも、急速な利用拡大とともに個人情報保護への様々な取り組みを迫られている。2015 年 8 月の時点で Facebook は 14 億 9,000 万人のユーザーが利用しており、現在、インターネット上で最もユーザー数が多い SNS となっている。Facebook は SNS 業界 2 位の中国のインスタントメッセンジャーTecent QQ（8 億 3,200 万人）を大きく引き離し、Twitter（3 億 1,600 万人）、Skype（3 億人）、LINE（2 億 1,100 万人）などよりもはるかに多くのユーザーを抱えているほか[47]、北米におけるモバイルデバイスからの通信トラフィックのうち Facebook が全体の 14.76%を占めるな

[43] 設定しておいたパスワードと、ログインのたびに異なるパスコードを入力する方法。Apple 社の場合、新しいデバイスから iCloud に接続しようとすると、登録しておいた iPhone にパスコードを送信する。これにより iCloud の不正ログインを防ぐというもの。
[44] http://www.informationweek.com/it-life/ios-9-android-m-place-new-focus-on-security-privacy/a/d-id/1321005?page_number=1
[45] http://techcrunch.com/2015/05/28/google-announces-android-m-with-fingerprint-scanner-support-android-pay-improved-permissions-battery-and-performance-tweaks/#.escsoo:mY0K
[46] http://www.apple.com/ios/whats-new/
http://bgr.com/2015/05/28/android-m-fingerprint-password-manager-app/
[47] http://www.statista.com/statistics/272014/global-social-networks-ranked-by-number-of-users/

ど、ユーザー数だけでなく利用も非常に多い SNS となっている[48]ため、業界や消費者も同社の個人情報保護への取り組みには大きく注目している。

図表 10 は、各 SNS のユーザー数となっている。

図表 10:各 SNS のユーザー数



出典:Statista を基に作成[49]

Facebook と個人情報の関係はなんといっても広告にある。同社の売り上げは 2014 年に初めて 100 億ドルを突破したが、その大部分が広告収入であり[50]、同社はユーザーへの効果的な広告戦略を推進する上で登録者データを使いユーザーの興味に基づく広告を表示させるターゲット広告という手法を取ってきた。2014 年 6 月には Facebook 上以外でのユーザーの行動データを使用することで、より精密なターゲット広告を行うことを発表した。これは、ウェブサイトに組み込まれた Facebook の「いいね！」ボタンや共有ボタンなどのソーシャルプラグインと呼ばれる機能を通して、ユーザーがボタンを押したかどうかにかかわらずウェブサイトを閲覧したことを確認し、ユーザーが閲覧したウェブサイトの情報と、Facebook 上のプロフィールや投稿からユーザーの好みを分析して広告戦略へ役立てるというものである。例えば、過去にラザニアが好きだと投稿していたユーザーが他のショッピングサイトで調理器具を検索した場合、そのユーザーには「ラザニアを盛り付けるのに便利な調理器具」の広告を表示するといった仕組みである[51]。Facebook を利用していないウェブ滞在時間のユーザーの行動までも追跡する形となるため、プライバシー面への懸念に対応するために、Facebook はウェブサイトとモバイルサービスの両方で外部データを使用した広告の表示をオフにできるようにしており、ユーザーにオプトアウトできる権利を用意している[52]。

図表 11 は、Facebook のソーシャルプラグインと広告設定の画面となっている。

[48] http://mashable.com/2014/05/14/youtube-facebook-mobile-traffic/#NKFrBNZr2kkC
[49] http://www.statista.com/statistics/272014/global-social-networks-ranked-by-number-of-users/
[50] http://mashable.com/2015/01/28/facebook-q4-earnings-2014/#fe2ibfli2GkI
[51] http://arstechnica.com/business/2014/06/facebook-brings-in-a-new-eerily-accurate-form-of-ad/
[52] http://www.smh.com.au/digital-life/digital-life-news/facebook-starts-using-your-web-browsing-history-to-target-ads-20150922-gjs0qw.html

図表 11：Facebook のソーシャルプラグイン（左）と広告設定の画面（右）

出典：The Sydney Morning Herald[53]、ITmedia[54]

しかしながら、2014 年 12 月、Facebook が広告戦略のためにプライベートメッセージの内容を読み取っていたことが発覚し、米国で集団訴訟に発展した。この問題は、2014 年 1 月にユーザー同士でやり取りしたプライベートメッセージ内で共有されたウェブサイトの URL を、Facebook が読み取り、ユーザーの好みを表す「いいね！（Like）」に追加してターゲット広告に利用していたというものである。2 人のユーザーが集団訴訟を求める訴えを起こしたことに対し、Facebook は訴えを却下するように連邦地方裁判所に要請していたが、連邦地方裁判所は Facebook の説明が十分でないとして Facebook 側の要請を棄却、集団訴訟で争われる運びになっている[55]。

このほか、Facebook は 2014 年 9 月に、Microsoft 社から前年に買収した広告プラットフォーム Atlas を活用していくことなども発表している。詳細は明らかにされていないものの、Atlas を活用することで広告を見たユーザーと外部のショッピングサイトでの購入を結びつけることが可能になり、広告の有効性を分析するものとされている[56]。2014 年 10 月には、自社データを活用することで広告枠を外部サイトに設置していくことを発表するなど、広告主 200 万社を持つ Facebook はユーザーのデータを用いた広告戦略を展開させており[57]、それと並行する形で個人情報の取り扱いに関する懸念もいまだに続いている。

[53] http://www.smh.com.au/digital-life/digital-life-news/facebook-starts-using-your-web-browsing-history-to-target-ads-20150922-gjs0qw.html
[54] http://www.itmedia.co.jp/news/articles/1509/18/news079.html
[55] http://www.bloomberg.com/news/articles/2014-12-24/facebook-fails-to-dismiss-privacy-case-over-messages
http://www.cnet.com/news/facebook-sued-for-allegedly-intercepting-private-messages/
[56] http://techcrunch.com/2014/09/28/facebook-atlas-relaunch/
http://www.wsj.com/articles/facebook-extends-reach-withad-platform-1411428726
[57] http://gizmodo.com/facebook-is-going-to-use-its-data-to-sell-ads-on-third-1640221469
http://techcrunch.com/2015/02/24/facebook-now-with-over-2-million-active-advertisers-launches-ads-manager-app-for-ios/

4　米国の個人情報保護に関する法律

（1） 米国における個人情報保護の法律

a. 個人情報保護に関連した連邦法

米国には個人情報保護する包括的な法律はないものの、時代の変化に合わせて各分野で個別に立法化する措置が取られてきた。1973 年ごろに携帯電話や電子メールの技術が確立し、1989 年にはインターネットの商用化が開始されたことから、それまでは IT 技術に対応した個人情報保護政策が取られてきた。その後はインターネットの普及とともに 1990 年代には電子データの取扱いに関する法律が導入され、同時多発テロの発生以降の 2000 年代は、国家安全保障のための個人識別と、個人識別が可能な情報の保護を目的とした法律が制定された[58]。

図表 12 は、米国における個人情報保護に関連した法律をまとめたものとなっている。

図表 12：米国における個人情報保護に関連した法律

年代	目的	法律（日本語）	法律（英語）	成立・改正年
1970 年代	プライバシー権利の確立	情報公開法	Freedom of Information Act	1974 年
	IT の発達に対応した法律	1974 年プライバシー法	Privacy Act of 1974	1974 年
		家族教育権とプライバシー法	Family Educational Rights and Privacy Act	1974 年
		外国情報監視法	Foreign Intelligence Surveillance Act	1978 年
	金融	公正信用報告法	Fair Credit Reporting Act	1970 年
		銀行秘密保護法	Bank Secrecy Act	1970 年
		金融プライバシー権法	Right to Financial Privacy Act	1978 年
1980 年代	個人情報保護の強化	電話加入者保護法	Telephone Consumer Protection Act	1991 年
1990 年代	個人情報保護の強化	ドライバー・個人情報保護法	Driver’s Privacy Protection Act	1994 年
		医療保険の携行性と責任に関する法律	Health Insurance Portability and Accountability Act	1996 年 2002 年
		児童オンライン 個人情報保護法	Children’s Online Privacy Act	1998 年
		金融サービス制度現代化法	Financial Modernization Services Act	1999 年
2000 年代	テロリズムへの対応	米国愛国者法	USA PATRIOT Act	2001 年
		国土安全保障法	Homeland Security Act	2002 年
		情報活動改革テロリズム予防法	Intelligence Reform and Terrorism Prevention Act	2004 年
		電子 ID カード法案	Real ID Act	2005 年

[58] http://www.gao.gov/assets/660/658151.pdf

	消費者のプライバシー	公正かつ正確な信用取引のための法律	Fair and Accurate Credit Transactions Act	2003 年
		医療保険の相互運用性と説明責任に関する法律	Health Information Technology for Economic and Clinical Health Act	2009 年

出典：A Brief History of Information Privacy Law を基に作成[59]

この中で、1996 年に成立した医療保険の携行性と責任に関する法律（Health Insurance Portability and Accountability Act：HIPAA）は、個人の医療データのプライバシーを守りつつ、データを医療の進歩に役立てることを目的とした法律となっており、医療分野に進出する IT 企業などが個人情報保護を重視した医療データの取り扱う際の基準として活用されている。例えば、IBM 社は人工知能 Watson を活用した医療プラットフォーム Watson Health Cloud を開始したが、HIPAA に準拠した医療データの取り扱いであることを全面に打ち出している[60]。HIPAA におけるプライバシールールでは、以下の場合のみ医療データを使用または開示することが認められる[61]。

- 医療データを提供した個人へデータを開示する場合。（情報開示の要求がない場合でも）
- 医療データを提供した個人への治療や支払い、医療に関連した行為を実行する場合。
- 医療データの使用や開示に関して、医療データを提供する個人への同意や反対の機会について話す場合。
- 許可された範囲での偶発的な使用や開示。例えば、待合室で健康状態を尋ねている際に、他の人が話しの内容を聞いてしまうといった場合[62]。
- 公共の利益や貢献につながる場合。
- 研究や公衆衛生などへの医療データの使用に対して、個人を特定することが可能な情報（名前、住所、家族構成など）を消去した限定的なデータを使用する場合。

患者の医療データを使用する原則として、匿名化された情報であるか、個人が特定可能なデータである場合には HIPAA のプライバシールールの範囲内かデータの提供者が文書で許可した範囲に限られている。当初の目的以外で医療データを使用する場合でも、プライバシールールの範囲内か、匿名化して使用する必要がある[63]。

b. オバマ政権における個人情報保護法（サイバーセキュリティ情報共有法（CISA）等）

オバマ政権における個人情報保護への取り組みは、スノーデン事件や多くの情報流出事件を受けて様々な法案の成立という形につながっている。オバマ大統領は 2012 年にビッグデータの研究開発を後押しするビッグデータ研究開発イニシアチブ（Big Data Research and Development Initiative）とともに消費者の個人情報保護を目的とした消費者プライバシー権利章典（Privacy Bill of Rights）を打ち出すなど[64]、もともと個人情報保護を重視する政策をとっていた。

[59] http://scholarship.law.gwu.edu/cgi/viewcontent.cgi?article=2076&context=faculty_publications
[60] http://www.prnewswire.com/news-releases/ibm-and-partners-to-transform-personal-health-with-watson-and-open-cloud-300065025.html
[61] http://www.hhs.gov/ocr/privacy/hipaa/understanding/summary/index.html
[62] http://www.hhs.gov/ocr/privacy/hipaa/understanding/coveredentities/incidentalusesanddisclosures.html
[63] http://www.hhs.gov/ocr/privacy/hipaa/understanding/summary/index.html
[64] https://www.whitehouse.gov/blog/2012/02/23/we-can-t-wait-obama-administration-calls-consumer-privacy-bill-rights-digital-age
https://www.whitehouse.gov/sites/default/files/microsites/ostp/big_data_press_release_final_2.pdf

しかしながら、2013 年 12 月に発生したスノーデン事件によって様々な通信を傍受していたことが暴露されると、2014 年 1 月に NSA の改革案を発表し[65]、同年 5 月には消費者のプライバシーを重視したビッグデータ政策に関する報告書を公表するなど[66]、個人情報保護について理解を求めた。そして 2014 年には、JP モルガン社、Target 社、米病院ネットワーク Community Health System などで情報流出が相次いだことにより、サイバーセキュリティや個人情報保護に関する問題に取り組むべく政策の策定に動きまわった。

2015 年 1 月の一般教書演説前にも、オバマ大統領は新しい個人情報保護に関する以下の個人情報保護の政策について発表している[67]。提案された法案は以下の通りである。

- Personal Data Notification and Protection Act(個人情報の通知と保護法):個人情報保護の新たな連邦基準を定める法案。データ漏えいの発覚後 30 日以内に、情報が流出したことを顧客に通知するよう企業に求める。

- Consumer Privacy Bill of Rights(消費者プライバシー権利章典):政権 1 期目に出されていた同法案の復活を目指す。自分たちのデータについて何を収集し、どのように共有するかコントロールする権利をインターネットユーザーに付与する内容。

- Student Data Privacy Act(学生データ保護法):教育現場にテクノロジーを持ち込む動きが加速する中で、テクノロジー企業が学生について収集したデータから利益を得ることを禁止する。同法案は 2015 年 5 月に Edward Markey 上院議員(民、マサチューセッツ州)と Orrin Hatch 上院議員(民、ユタ州)から提出されている[68]。

そして 2015 年 4 月、サイバー攻撃による個人情報保護を目的としたサイバーセキュリティ情報共有法(Cybersecurity Information Sharing Act:CISA)案が連邦議会の下院を通過し上院に送られた[69]。この法案は、スノーデン事件を受けて 2013 年に出された法案を更新したものとなっており、政府と企業がインターネットのアクセス状況やサイバー攻撃の情報共有を目的としている。ただし、同法案ではサイバー攻撃の情報共有が目的となっているが、企業が情報を提供することに対して訴訟などから守られることが盛り込まれているため、個人のプライバシーが保護されていないのではないかという声が上がっている[70]。

(2) 州政府の取り組み

米国では州によって独自の判断の個人情報保護に関する法律が作られている。いくつかの州政府は、連邦法では盛り込めない具体的な内容を補う形で州法を制定することが多く、オンライン上の犯罪など州の境界を越えた犯罪や各州で声が上がっている問題に取り込むために、様々な独自の個人情報保護に関する法が作られている[71]。

- 米 47 州とワシントン DC: Security Breach Notification Laws

[65] http://www.washingtonpost.com/politics/full-text-of-president-obamas-jan-17-speech-on-nsa-reforms/2014/01/17/fa33590a-7f8c-11e3-9556-4a4bf7bcbd84_story.html
[66] https://www.eff.org/deeplinks/2014/05/white-house-big-data-report-good-bad-and-missing
[67] http://www.zdnet.com/article/obama-calls-for-new-privacy-laws-including-mandatory-hack-notifications-within-30-days/
[68] http://www.businessinsider.com/student-are-unwittingly-volunteering-personal-information-lawmakers-say-2015-5
[69] http://www.usnews.com/news/articles/2015/04/22/house-approves-controversial-cybersecurity-bill
[70] http://www.forbes.com/sites/gregorymcneal/2014/07/09/controversial-cybersecurity-bill-known-as-cisa-advances-out-of-senate-committee/
https://www.eff.org/ja/deeplinks/2015/08/obama-administration-supports-privacy-invasive-cybersecurity-bills
[71] http://www.nytimes.com/2013/10/31/technology/no-us-action-so-states-move-on-privacy-law.html?_r=0

米 47 州とワシントン D.C.は、個人情報などを含む情報漏えいが発覚した際には、被害者への通知を義務付ける法令を成立させている。各州などで法令の内容は異なるが、主に法令に準拠しなければならない機関や団体の特定、「個人情報」の定義、「侵害」にあたる行為の特定の通知方法、適用除外から構成されている。フロリダ州の法令は特に厳しいものとなっており、2014 年 7 月から施行された 2014 年フロリダ情報保護法（Florida information protection act of 2014）では、国外の企業であってもフロリダ州の住民の個人情報を流出させた場合には州政府などへの報告義務が課せられるというものである[72]。現在、全米で同様の法律を制定させていない州は、アラバマ州、ニューメキシコ州、サウスダコタ州となっている[73]。

- バージニア州：SB 1275 Medical data in an electronic or digital format; limitations on use, storage, sharing, and processing
  10,000 人以上の患者の個人情報を電子フォーマットまたはデジタルフォーマットで保存している医療機関もしくはそれに準ずる機関に対して、データベースのアクセスを規制する内容。医療情報の共有に患者が同意したとしても、それを医療関係者以外への電子フォーマットまたはデジタルフォーマットでのデータの転送などに同意したとみなしてはならないと定めている[74]。

- カリフォルニア州：California's Privacy Rights for California Minors in the Digital World Act
  カリフォルニア在住の未成年者が、インターネット上のウェブサイト、オンラインサービス、アプリに掲載されている情報の削除を要請できることを保証する法令。また未成年者の個人情報を元にして特定の商品をマーケティングしたり、告知したりすることを禁じている。

- コネチカット州：Safeguarding of personal information. Social Security numbers. Privacy protection policy
  ビジネスにおける過程で顧客から社会保障番号を預かる企業は、個人情報保護のポリシーを設定し、ウェブサイトなど公の場所に掲示しなければならない。また社会保障番号の秘密保持を保証すること、そしてその不正な開示を禁じることを明らかにしている[75]。

[72] http://www.mondaq.com/unitedstates/x/327078/data+protection/New+Florida+Information+Protection+Act+Expands+Data+Breach+Notification+Requirements
[73] http://www.ncsl.org/research/telecommunications-and-information-technology/security-breach-notification-laws.aspx
[74] http://lis.virginia.gov/cgi-bin/legp604.exe?131+sum+SB1275
[75] https://www.cga.ct.gov/2011/pub/chap743dd.htm#Sec42-471.htm

5　個人情報に関連する最先端技術

（1）　個人情報保護対応スマートフォン Blackphone 2

スイスのスマートフォンメーカーSilent Circle 社が開発する BlackPhone 2 は、個人情報保護を重視したスマートフォンとなっている。同製品はソフトウェア面での強化に特に力を入れており、OS には Android をベースとした独自の Silent OS を採用している。Silent OS には OS レベルで複数の仮想領域を管理する機能 Spaces が搭載されており、1 台のスマートフォンの中で異なる OS の利用環境を作り出せる点が特徴となっている。仮想領域の間は一切のデータが共有されないため、会社用とプライベート用などに使い分けることができ、データを切り分けるために 2 台のスマートフォンを所有する必要がなくなる。このため、個人所有のデバイスを業務に持ち込む BYOD（Bring Your Own Device）を導入する企業などでの活用が期待されている[76]。

このほか、BlackPhone 2 には暗号化された通信を提供するアプリ Silent Phone が搭載され、安全な通話、ビデオ電話、テキストメッセージが可能となっている。Android をベースとしているため、Google Play からのアプリ購入、Gmail などの Google 社のモバイルサービスや BYOD 向けアプリ Google for Work など、通常のスマートフォン向けサービスも利用できる。2015 年 7 月には Silent Circle 社が Android for Work の開発パートナー企業として参加することが発表された。BlackPhone 2 は 9 月中には価格などの詳細を発表する予定となっている[77]。

図表 13 は、Silent Circle 社の BlackPhone 2 となっている。

図表 13：BlackPhone 2

出典：Silent Circle[78]

[76] https://www.silentcircle.com/products-and-solutions/devices/silent-os/
http://gizmodo.com/the-best-phones-for-the-privacy-obsessed-1715856498
[77] http://techcrunch.com/2015/07/30/google-adds-8-carriers-to-its-android-for-work-partner-ecosystem/
[78] https://www.silentcircle.com/products-and-solutions/devices/silent-os/

（2） 個人情報保護対応教育アプリ管理プラットフォーム

Clever 社では学校で使われる教育系アプリを一括管理できるプラットフォームサービスを提供する上で、教育現場における生徒の個人情報保護に取り組んでいる。米国の学校の教育現場では、様々なアプリやサービスを使って授業や生徒のデータが管理されているが、サービスの中には生徒の名前や年齢だけでなく、生徒の学習レベルや宿題を提出したかどうかなど詳しいデータを取り扱ったものもある。このため、同社は学校のデータベースとアプリを提供する企業の間に入り、アプリがどのようなデータを学校のデータベースから使用しているか監視するとともに、データの使用がセキュリティやプライバシーポリシーに乗っ取ったものであるかをチェックできるプラットフォームサービスを提供している。また、地域の学校を管理する機関が、教師がどのアプリを使いデータの取り扱いを誤っていないか確認できる機能もあり、同社のプラットフォームサービスは生徒の個人情報保護に向けて様々な対応が行われている[79]。

図表 14 は、Clever 社の教育アプリ管理プラットフォームサービスを表したものとなっている。

図表 14：Clever 社の教育アプリプラットフォームサービス

出典：Clever[80]

Clever 社のプラットフォームサービスの大きな特徴は、学校側がサービスを無料で利用できるという点である。Clever 社はプラットフォームを使用するための API を提供するだけであり、個々の教育アプリ提供事業者から学校数に応じて 1 校ごとに 5 ドル～25 ドルのライセンス料を受け取ることで、収益を確保する形となっている。学校側には Clever 社のプラットフォームサービスを利用する際の料金がかからないため、利用する学校が大きく増え、現在では全米の学校の 3 分の 1 にあたる 44,000 校が同社のサービスを利用しているとされている。また、学校側ではアプリごとにログインする必要がなく、Clever 社のプラットフォームを通して一括ログインできるシングルサインオンとなっている点なども、学校側の利用を大幅に向上させる大きな要因になっている[81]。

[79] http://www.buzzfeed.com/mollyhensleyclancy/clever-secures-students-data#.oaYYLIYDv2
[80] https://clever.com/
[81] http://blogs.wsj.com/venturecapital/2014/12/16/clever-raises-30-million-for-single-login-education-tech-app/

（3） 次世代の 3D 対応指紋認証技術

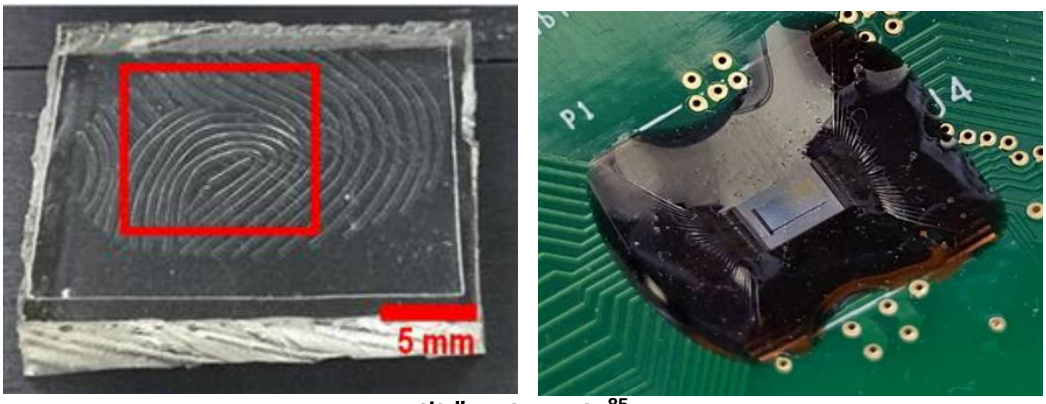
スマートフォンなど様々な機器に搭載されるようになった指紋認証技術であるが、セキュリティのハッキングが続いており、セキュリティ面への懸念は後を絶たない。具体的には、人工的に作ったニセの指紋を使い iPhone の指紋認証のセキュリティが破られた例や[82]、政治家の写真から指紋を読み取って複製することに成功した例が現れており[83]、指紋認証のセキュリティを破る手法は高度化してきている。

そうした中、これまで以上の高度なセキュリティを持った指紋認証技術の研究が進められている。2015 年 7 月にカリフォルニア大学 Davis 校が研究開発した新しい指紋認証技術は、指紋の模様だけでなく、指紋の凸凹まで読み込む 3D 指紋認証となっている。この技術は、超音波を使うことで指紋の凹凸を立体的に読み込むことが可能であり、より高いセキュリティを持った指紋認証が可能となっている。

この 3D 認証には最新の医療機器の技術が応用され、すでにスマートフォンなどに搭載できるほど小型化され、しかも省電力で動作するという。さらに、複数の周波数を使用することで皮膚の下まで見ることが可能であるため、医療への応用も期待されている。民生用の超音波スキャナーの製造は難易度が高いため、大量生産の方法が 3D 指紋認証スキャナーの今後の課題となっている[84]。

図表 15 は、3D 指紋認証スキャナーと撮影画像となっている。

図表 15：3D 指紋認証スキャナー



出典：Gizmodo[85]

[82] http://www.dailymail.co.uk/sciencetech/article-2889860/Hackers-steal-fingerprint-PHOTO-Copycat-print-used-criminals-fool-security-systems.html
[83] http://news.softpedia.com/news/Hacker-Copies-Fingerprint-of-German-Defense-Minister-from-Public-Photos-468459.shtml
[84] http://gizmodo.com/3d-fingerprint-scans-could-be-the-ultimate-security-too-1715134095
http://www.nature.com/news/ultrasound-fingerprint-scanners-amplify-security-1.17904
[85] http://gizmodo.com/3d-fingerprint-scans-could-be-the-ultimate-security-too-1715134095

6 終わりに

IoT やビッグデータ、そして人工知能など、先端 IT を活用したビジネスが大きく拡大していくことで、我々の生活は一層便利で快適なものになり、また新しいビジネス・モデルも次々と誕生してくるなど、データを活用したビジネスは将来の発展を大きく期待させるものである。他方、扱う個人情報が多くなり、また広範に活用されることで、今回取り上げた個人情報保護の問題は益々重要になってくる。
個人情報保護の取り組みを強めれば強めるほど、利便性や今後の発展性には悪影響を与えることから、どのように両者のバランスを取っていくかは難しい課題といえる。しかし今回紹介したように、新しい技術を開発することで個人情報保護を強化する動きもあるように、ここから新しいビジネスが誕生してくることも考えられる。
日本と米国では、個人情報保護に関する取り組みや考えは異なるものの、米国の IT ビジネスにおける個人情報保護の取り組みや技術開発、そして法律制定の動きは今後も注視していくことが大切であろう。