博士論文

バランスのとれた個人情報保護規範の実現に向けて

－情報セキュリティ事故が避けられない時代の、

不適正な流通の検知と執行強化による

消費者保護－

Keiko Kaneko

金子啓子

情報セキュリティ大学院大学

情報セキュリティ研究科

情報セキュリティ専攻

2017 年 9 月

内容

1　はじめに

1.1 問題意識

日本において、個人情報保護規範の最強のエンフォースメントはレピュテーションリスクである。

真面目な企業は、この最強の強制力を恐れ、また、日本特有の顧客至上主義も相まって、顧客向けの宛名が書かれた伝票 1 枚でもきっちり管理し、紛失した時には、お客様にお詫びする。また、いわゆる萎縮効果により、法律上違法ではないと解釈できる範囲であっても慎重になり、ICT の発達に伴う新しいサービスにも尻込みしがちである。

一方、経済合理性の範囲とはいえ情報セキュリティ対策に真面目に努力していても、技術の発達や攻撃方法の急速な発達、攻撃ツールの流通や攻撃者の組織化などにより、漏えいを完全に防ぐことは不可能になりつつある。しかし、ひとたび漏えい事故が起こると、漏えいした事業者は社会や顧客からの信頼を失い、時には個人情報保護法に基づく処分を受ける。漏えいされた個人は、見知らぬ事業者に自分の情報が渡ったことはプライバシー侵害である、として、漏えいした事業者に損害賠償請求し、判例でも慰謝料が認められてきている。これがまた、他の真面目な事業者の萎縮につながる。

しかし、窃取され、漏えいした情報を売買する名簿販売事業者や名簿販売事業者から買い取り情報を利用する事業者には、行政の調査もなければ、社会的非難も強くない。これらの事業者には、レピュテーションリスクも気にしない事業者も多く、消費者は本人関与の権利を行使してコンタクトすることも躊躇する。見知らぬ事業者に渡った情報を少しでも削除させるなどコントロールしようとする努力は、漏えいした事業者が営業秘密に基づいて地道に警告することがあるくらいで、個人情報保護法に基づく調査などは行われていない。

これで、消費者は守れるのだろうか？なぜこのような秩序なのか？　消費者を守り、真面目な事業者が萎縮しない、もっと合理的でフェアで実効性のある個人情報保護規範を築けないだろうか。

1.2 この論文の位置づけ

1.2.1 個人情報保護規範の役割と発展

個人情報保護法の分野は、技術の発展と法、人権理念先行型の欧州とプラグマティックな米国との知的で政治的な確執等、知的好奇心を満たす分野である。多くの論文がこれを華々しく議論し、規範が形成されてきている。

言うまでもなく、個人情報保護規範は、情報の伝達や情報通信技術の発展とそれに伴う社会の変化に伴って出現し、発展してきた。19 世紀末、アメリカで初めてプライバシーの権利を認めた判決は、新聞広告に無断で肖像を使われたケースからだった。新聞による情報の伝達が権利性まで認めさせた、といえる。

1970 年代の欧州と米国での（カバレッジが違うとはいえ）個人情報保護法の制定も、コンピュータの発展により、政府や大企業での電算化が進み、所謂、ビッグブラザーへの懸念か

ら、少なくとも政府の手を縛るために、個人情報保護の取扱のあるべき秩序を示そうとしたものである。

元々、大陸法は、英米法に比べて概念から入る傾向があるが、欧州は、ナチスドイツ時代の反省もあり、個人情報保護を人権に立脚する形で法制化した。このため、当然、対象は、政府だけでなく、すべての人であった。一方、英米法は、本来、判例法の蓄積と権力の手を縛るマグナカルタから発展している。英国の権力から独立してできた米国の憲法は、基本的には権力の手を縛る発想でできている。政府の手を縛る法規範には関心があるが、一方で、通信販売業者などの力が強く、電算化で世界を制覇するコンピュータメーカーを擁していた米国では、まず、政府を対象としたプライバシー法を制定した。その後、必要が出た都度、事業セクターごとの法律を制定している。

そして、1970 年代のこの両地域の法規範の違いの裏には、欧州諸国の、米国の強力なコンピュータメーカーの独占による支配に対するけん制の目的もあった。よく知られているように、1980 年の OECD ガイドラインもこの両地域の妥協からできたものである。

その後米国は、1992 年、WTO を通じて、TRIPS や TRIM のように、直接貿易対象となるものではない国内秩序に関する規範を、大きな市場と有利な貿易を得るための条件として加盟国に要求する方法で広げようとした。一方、EU は、指令の中に、相互主義を入れることによって、自らと同様の規範を広げようとした。1995 年の個人情報保護指令はその一つであり、背景には、前述の、米国との確執がある。

このような 1990 年代は、インターネットが劇的に普及・発達し、社会に影響を及ぼし始めた時期でもある。欧州は 1995 年の指令の各国法化と並行して、2002 年、e プライバシー指令を成立させ、通信行政の切り口からこの問題に対処しようとした。その後のインターネットが及ぼす社会的な変化に対応すべく、2009 年に e プライバシー指令を改訂している。一方、米国では、法規制で守るのではなく、認証や技術などの自主的な対応でこの技術と社会の変化に対応し、新たなビジネスの出現を阻害しないようにするアプローチを取った。FTC が、各社が Web サイトに掲出するプライバシーポリシーを利用して、言明責任に基づき消費者の個人情報保護規範の enforce を始めた。

2010 年以降、FTC は enforce の範囲を広げ、今では、プライバシーポリシーがなくても、セキュリティ侵害について消費者に対する欺瞞的商行為、として enforce するようになっている。また、技術的発展に対しては、FTC の規則制定権限に基づき、様々なガイドラインを制定して、新たな問題への指針を示している。更に、2012 年には、オバマ大統領も、Consumer Privacy Bill of Rights を公表し、立法化を要請している。

一方、欧州では、指令の適用の範囲の事項については EU の第 29 条作業委員会が解釈や指針を出すことによって、技術や社会の進化に対応していった。そして、Google、Amazon などの米国企業が直接 Web サイトなどを通じて欧州の個人に関する情報を収集、利用し、また、インターネットを利用した様々なサービスを直接欧州に提供することにより、個人や個人が特定されなくても個々の人を識別した行動履歴などが収集されることに対応し、また、指令による各国ごとの官僚的な対応の限界を克服し、インターネットのない時代に策定された指令から現代の状況に合わせるべく、2012 年 1 月、欧州委員会は個人情報保護規則案を提案し、2016 年 4 月一般データ保護規則が制定された。

このように、個人情報保護規範には、情報通信技術の発展とそれに伴う社会の変化に伴っ

て、指針を示す役割が大きい。

1.2.2 個人情報保護規範の執行上の問題

個人情報保護法は、前述の技術の発展と社会の変化への対応のためには、実際上、地道な執行は、不要である。

ガイドラインなどの試案公表の段階で、大まかな方向性は示され、普通の事業者なら、そこで問題とならない方法を考える。しかし、本質的に、ガイドラインは、技術の発展とサービスの出現を後追いするものである。指針のない先駆的な事例が発生すれば、マスコミでも取り上げ、個人情報保護法やプライバシーとの関係を問題にする。それを追いかけて、当局がヒアリングし、事業者はプライバシー上、問題のないやり方に変えたり、当局が追いかけてガイドラインを出したりする。また、特に欧州の当局はガイドラインがなくても理由を付けて、規制したりすることもある。

例えば、Google がストリートビューを始めたころは、欧州でも日本でも、個人情報保護法、プライバシーとの関係がマスコミ等で問題となったが、Google も初めから削除要請受付等をアナウンスしていたことから、何とか問題にしたい当局との微妙な確執となった。例えば、2009 年、Google は、ルクセンブルグの個人情報保護当局に、グーグルストリートビューと個人情報保護法の関連についての質問をしている[1]。ルクセンブルグ当局は、複数の国の個人情報保護当局が 2009 年 2 月に採択した共同ポジションに従い、個人情報保護法上の本人の権利を厳格に守るよう要請し、簡単に本人が削除要請できるようにする条件を付けた。しかし、同年 5 月、予め撮影する場所と期間を全国メディアやインターネット上に告知しなかったとして、撮影を中止させ、是正後、同年 8 月、再開を許可するなどしている。日本においても、システム会社が鉄道乗降情報を利用したサービスの企画をアナウンスした途端、マスコミ等で大きな問題となり、法改正に至っている。米国では、元々、セキュリティポリシーと技術的な対応でプライバシーを守るという観点から、FTC は事業者たちと連携して、早い段階で指針を出すなどしている。

日本では、真面目な事業者は、マスコミが批判することで萎縮して慎重になるため、執行は不要である。米国の大きな企業は目立つため、地道な執行は不要であり、むしろ、「罰金もコスト」と割り切れる財力のある企業にどのように実効性を持たせるか、が、課題となる。

このような先進的な事例は、前向きな話であり、知的好奇心を満たし、創造的な立論が可能なため、学者も注目し、華々しく議論されている。

しかし、多くの消費者たちが不安に思い、迷惑を被っているのは、このような先進的な事例ではなく、個人情報保護への基本的な懸念である。本人の知らないところで個人情報が売買されていることを不安に思い、心当たりのない勧誘電話に迷惑を被っている。また、クレ

[1] EU 第 29 条作業委員会, Thirteenth Annual Report of the Article 29 Working Party on Data Protection, 2010 年 7 月 14 日 http://ec.europa.eu/justice/data-protection/article-29/documentation/annual-report/files/2010/13th_annual_report_en.pdf (2017･5)

ジットカード番号などの流出により、個人又はクレジットカード会社に経済的被害が発生している。このような不正な流通に対する執行は、端緒となる情報収集と地道な調査が必要であり、実効的な執行があまり行われていない。

個人情報の売買は、網羅的な個人情報保護法のない米国では合法であり、大規模なデータブローカーがビジネスを行っている。全世界で 7 億人分のデータとほぼすべての米国消費者に関するデータを持つ会社や、ほぼすべての米国世帯の情報をマーケディングデータとして提供する会社、などがある。FTC も問題視し、2012 年、2014 年の 2 回に亘り、データブローカーの実態についての報告書を出して、立法的対応を要請しているが、未だに変化はない。

また、日本においても名簿販売事業者規制は少なくとも 2015 年改正法前は弱く、取扱量が減少したとはいえ残っている。名簿販売事業者については、消費者への詐欺のターゲットのリストを闇で販売するような「カモリスト」を取引し、詐欺等の犯罪行為に加担し、また不適切な勧誘等による消費者被害を助長する者もいるとして、社会問題として指摘されてもいる。そんな中、2014 年、内部者犯行による大規模な個人情報漏えい事件において、データが名簿販売事業者に売られ、競合する企業などが買い取って利用する実態が明るみに出て、改めて、消費者に、自分の知らないところで信用できるかどうかわからない見知らぬ事業者に自分や家族の個人情報が売られ、利用されていることへの不安が高まった。この事件により改めて、そのような流通の存在が、意図的な窃取を助長している面も浮き彫りになり、2015 年の個人情報保護法改正で対策が強化された。

このような流通に対しては、今まで、日本の個人情報保護法の調査の対象となったことがない。端緒があっても、そこから一つひとつ事業者を遡って確認しなければならない地道な調査が必要で、主務大臣制ではそれだけの調査体制が整えられなかった。むしろ、個人情報を漏えいしてしまった企業の報告や公表に対し法律上の勧告措置を行い、マスコミも漏えいした企業を批判することで、社会に安全管理を徹底させる圧力としてきた。流通する者、購入する者については、ほとんど批判されていない。

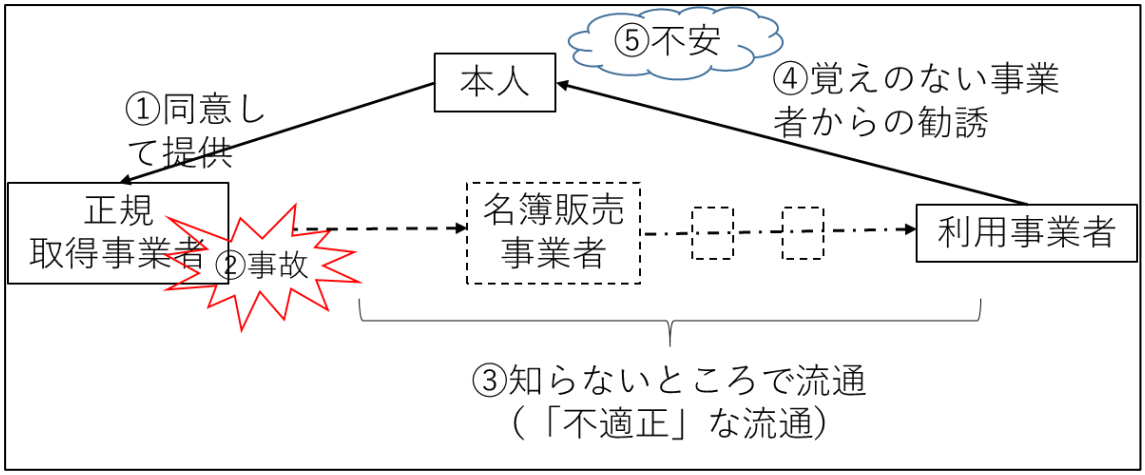


図 1　問題の構図

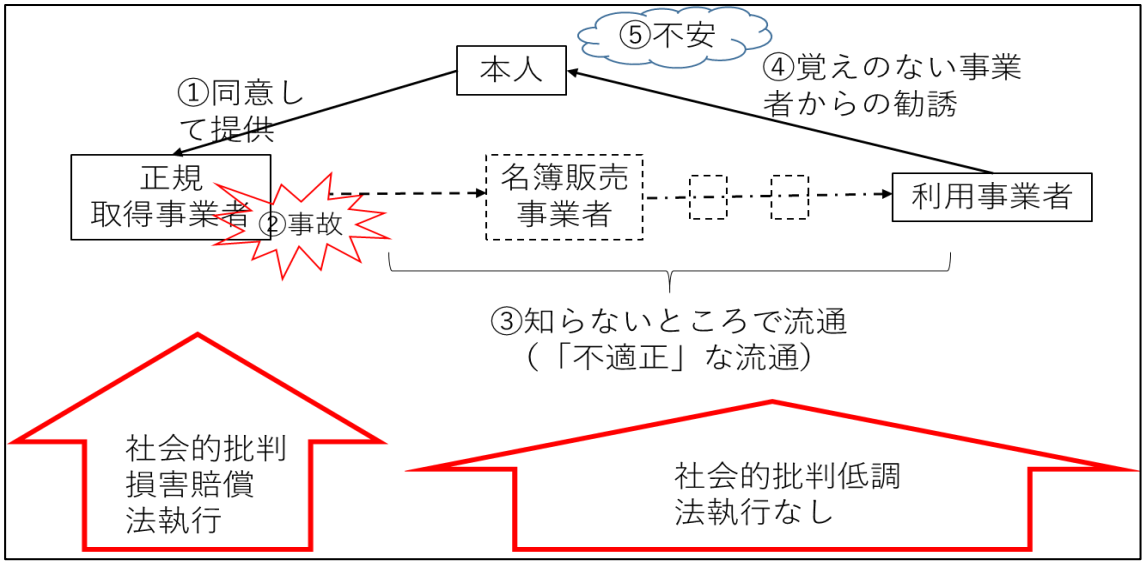


図 2　日本の現状

この問題が技術の発展と無縁という訳ではない。標的型攻撃など、インターネットから、意図的に目的の情報を窃取する技術と攻撃方法が発達し、気づかないうちに大量の個人情報を窃取されるようになっている。内部者犯行においても、対策の技術的な穴を探して持ち出すため、技術の発展に対策が追いついていない盲点があればそこから窃取される。このように、鼬ごっこの中、漏えいを完全に防止することは不可能といえる。

個人情報が漏えいした時に本人に知らせて自衛を促す侵害通知という制度がある。しかし、正規の事業者が気付かないうちに個人情報を窃取できるということは、侵害通知もできず、個人が自衛できないことにもなる。

気付かないうちに取られた情報を見つけるには、その情報が使われていることを検知するしかない。使用を検知し、「不適正」な流通を見つけ、法執行し、少しでも流出した情報を削除させコントロールすることができないだろうか。

国家による犯罪、ダークウェブの存在など、個人情報の不正な流通を完全に無くすことができないことは承知している。しかし、全く、手をこまねいているのではなく、検知力を高め執行力を上げなければ、正直者が馬鹿を見るだけの法律になってしまう。

この論文では、この地道な執行の課題に目を向けて、課題を整理し、改善のための提案を行いたい。

1.3 本論文の検討の枠組みと構成

本論文では、日本の個人情報保護規範の課題を整理し、主にプラグマティックな米国との比較で分析する。

また、図 3 のように、各論点は、漏えいした事業者に対する論点を「上流」、名簿販売事業者など流通者に対する論点を「中流」、流通した個人情報の利用を「下流」として分類する。また、図 3 の番号は、;

①本人から取得した事業者（内、漏えい事故を起こした取得事業者を②漏えいした事業者とも言及）、
③名簿販売事業者などの不適正な流通事業者
④そこから買い取って利用する事業者、

と、関係する当事者への言及に使用する。

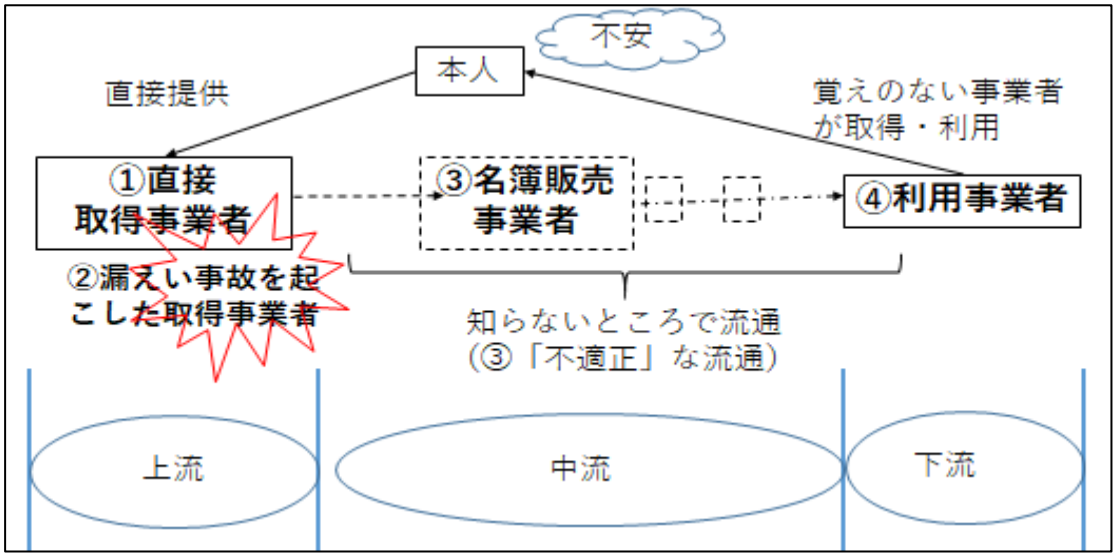


図 3　検討の枠組み

「上流」は主に漏えいした事業者への対応である。
①の正当に収集した事業者でも、事故を起こすと、通常、下記の影響がありうる；
(1)顧客と社会からの信用失墜
(2)侵害通知
本人通知
公表
官庁報告、認定個人情報保護団体報告
P マーク制度に基づく報告
(3)個人情報保護関連法の措置
(4)「お詫びのしるし」
(5)損害賠償訴訟
「中流」は、名簿販売事業者、（米国ではデータブローカー）の扱い
「下流」は、利用の法的評価と、利用の検知がある。

本論文では、まず、第 2 章で、日本の状況について、侵害通知を除く論点を整理する。
侵害通知については、第 3 章で、米国、欧州との比較で論じる。
第 4 章では、米国の個人情報保護法制を整理する。

第5章では、日米の事故実績を比較し、そこから推定される事故の検知能力の差を考える。

第6章では、比較に基づく小括と、そこで見えた課題解決に向けて、主に消費者保護法的制度である不招請勧誘規制制度を紹介し、その個人情報保護法制上の活用の兆しを紹介する。

第7章では、これらを踏まえて、日本における、より消費者が安心できる個人情報保護法の制度運用を提案する。

2　日本における個人情報保護規範の「執行」状況

2.1 日本の個人情報保護規範の特徴と背景

日本においては、個人情報保護法の成立後、「過剰反応」と言われるほど、人々は個人情報に神経質になったといわれる。すでに述べたように、経済合理性の範囲で最大限の情報セキュリティ対策を行っていても、完全に被害を防ぐことはほとんど不可能である、にもかかわらず、サイバー攻撃を受けて個人情報を漏洩・流出させた企業や団体は、個人情報保護の観点からは、被害者でなく加害者という立場で扱われることが多い。なぜなら、アタック自体の被害者ではあっても、預かっていた個人情報をアタックによって外部に流出・漏洩させたことによって、個人情報の本人に対しては加害者という立場になってしまうからである。特に、日本においては、マスコミからそのような観点で強く非難されることが多い。これはなぜだろうか。

そもそも日本人は、プライバシーに敏感だったのだろうか。

歴史的にみて、日本において、プライバシーの感覚が普及したのは第二次世界大戦後である。戦後、米国主導による社会・政治・経済体制の刷新と米国の文化の流入で、個人主義が少しずつ広まっていったが、それまでは、まだ、「むら社会」といわれるように、共同体の秩序が規範であり、「恥」や「村八分」が規範の強制力だった。共同体のメンバーについては、お互いにすべてを知っていることが当たり前であった。また、その起源は 7 世紀に遡ることができる戸籍制度の下、「お上」（国家）が個人個人を管理する長い歴史もある。

1964 年、東京地方裁判所が初めてプライバシーの権利を実質的に承認した[2]ことから、急速にプライバシーが注目を浴びるようになった。それでも、個人情報保護法の施行より後の 2006 年まで、住民基本台帳の閲覧・書き写しが可能であった[3]ように、プライバシーや個人情報の保護が国民の中に浸透・定着するにはかなりの時間がかかっている。

一方、1970 年、電算化推進の一環として各省庁に統一的な事務処理用個人コードを設定する制度を導入しようとした際、「国民総背番号制」であるとして、マスコミを中心とした世論の反発により、中止に至った[4]。　1970 年といえば、60 年代からの学生運動が過激になり、警察・公安の取締も強化された時代背景もあり、第二次世界大戦中の特別高等警察による思想弾圧の記憶の残るマスコミと国民が危うさを感じたのかもしれない。後述するように、この時のマスコミの「正義感」が、この後も日本の個人情報保護法の実質的な強制力に影響を与えているように思われる。

この反発を踏まえ、政府は、1975 年「行政機関等における電子計算機利用に伴うプライバシー保護に関する制度の在り方についての中間報告」を出したが、引き続き検討、と先送りの結論だった。[5]　しかし、その後の情報化の進展に伴い、1999 年、政府が住民基本台帳をネットワーク化（以下「住基ネット」）しようとした時までには、状況がかなり変わっていた。

世界的に進む電算化を受けた米国や西欧の動きを受け、1980 年、有名な OECD ガイドライ

---

[2] 「宴のあと」事件　（東京地判昭 39・9・28 判時 385・12）

[3] 住民基本台帳法の一部を改正する法律により、2006 年 11 月 1 日から閲覧可能な場合が限定された。

[4] 岡村久道『個人情報保護法〔新訂版〕』17 頁（商事法務、2009 年）

[5] 岡村・前掲注 4　17 頁

ン（「プライバシー保護と個人データの流通についてのガイドラインに関する理事会勧告」）[6]が採択されると、これに対応すべく、日本でも 1988 年、官のみを対象とする旧行政機関法（「行政機関の保有する電算機処理にかかる個人情報の保護に関する法律」）が成立した。民間については、通信、金融等の分野で主管省庁がガイドラインを策定し、行政指導的に業界団体などを通じて緩やかな適用を行っていたが、この頃は、一般の国民がそれほど個人情報に神経質になることはなかった。

1980 年代終盤、経済的に強力になった日本に対する米国の圧力[7]が高まり、官が民間を指導して国際競争力をつけ、外国企業の参入を難しくしているのがアンフェアであるという理論で圧力をかけ、このため日本では規制緩和が進んだ。加えて行政指導で独禁法違反は免責されないという判決[8]を背景に行政が抑制的になり、事前規制から事後規制へと自己責任化が進んだ。

更に、1990 年代のネットワーク社会の始まりから、情報化社会化に伴う法制は、米国のようになるべく規制や執行を少なくし、情報の自由な利用、技術、ビジネスの発展を促進するスタンスを取り、犯罪対策のような法規制の必要なものを除けば自主規制や市場の力に任せる流れがあった。

例えば、電子商取引などについて、インターネット内は現実の世界と全く違うので、従来の法律を適用すべきでなく法律を別に作るべき、という議論があった。しかし、日本は、ローマ法から続く人類の知恵がつまった民法・商法を当てはめればよく、混乱を心配するなら、その当てはめ方の解釈を整理し、それでも立法的に対応せざるを得ない点だけ立法的に解決する、というアプローチを取った。具体的には、経済産業省が有識者を集めて「電子商取引及び情報財取引等に関する準則」を出す形で対応した。準則は、その後も、技術や新しいサービスの出現に伴って定期的に改定されている。一方、米国では、情報財取引のための UCC（Uniform Commercial Code）を作成しようとして、UCC2B を作成し、その後 UCITA（Uniform Computer Information Transactions Act）として公表したが、採用した州が極端に少なく、挫折している。

こんな中、日本では、1995 年の EU 個人情報保護指令の相互主義条項[9]をきっかけに、個人情報保護秩序をどうするかの議論が再開された。地方公共団体レベルでは、個人情報保護条例を制定する動きが始まったが、国レベルでは、前述した情報化社会化法制についての方針の下、法制化よりも、米国の BBB オンラインや TRUSTe に倣ったシールプログラムによる保護を優先した。こうして 1998 年、「プライバシーマーク制度」[10]ができた。このように、民間については米国的アプローチを進めていた時期に、1999 年春、前述の住基ネット導入に向け

6　欧米でも国家が事務処理の電算化を進めることへの懸念が高まり、1970 年代には西欧の各国で個人情報保護法が成立し、米国では 1974 年に連邦の政府部門を対象とするプライバシー法が成立した。官民ともに包括的に対象とする欧州と、官のみを対象とし産業界に配慮し民間は必要が生じた分野でのみ立法するセクトラルアプローチを取る米国との利害対立もあり、OECD で利害調整された結果、このガイドラインが採択された。

7 米国議会は、日本を念頭に、包括通商法（Omnibus Trade and Competitiveness Act of 1988 , Pub.L. 100–418, AUG. 23, 1988, 102 Stat. 1107）により、優先的に交渉すべき国の慣行を特定し通商法 301 条に基づく交渉を行い、是正されないときは報復措置を発動する、という内政干渉的内容のスーパー301 条を成立させたりした。

8 石油価格カルテル事件　最高裁判所 1982 年年 3 月 9 日頁

9 The European Union Directive 95/46/EC　第 25 条

10 1999 年には日本工業規格として JIS Q 15001「個人情報に関するコンプライアンス・プログラムの要求事項」が制定され、プライバシーマーク制度はこれへの適合性評価制度となった。

た住民基本台帳法改正案が国会に提出された。

初めは 1970 年と同様、マスコミは「正義感」に基づきプライバシーを理由に反対したが、既に官を縛る旧行政機関法は運用されており、1999 年 5 月に発生した宇治市の住民基本台帳大量漏えい事件[11]などを契機に、「正義感」は、国、地方公共団体、事業者の安全管理や、名簿販売事業者や DM 事業者などに対し強制力のある法律が必要という主張に向かった。政府もうまく利用し、民間部門への漏えいの対処などを理由に「個人情報の保護に万全を期するために、速やかに、所要の措置を講ずるものとする」という附則をつけて住民基本台帳法改正案を成立させ、その附則に従い、紆余曲折[12]を経て 2003 年 5 月、官民ともに適用される包括的な個人情報保護法と関係の法律が成立した[13]。

このような背景から、日本においては 2000 年代から個人情報漏えい事故に対する報道は漏えい事故を起こした（遭った）企業に厳しいものとなり、非難に近いようなものとなったと考えられる。もちろん、企業は漏えいしないような対策をする義務があるが、時として、企業が結果責任を負わされているようにも見える。

筆者は、これが日本における過剰反応の理由ではないかと考える。更に、2.2 節で述べる損害賠償の状況も拍車をかけている。変化はしているものの、前述のように、日本社会の規範感覚は法律よりも共同体で「恥ずかしくない」か、非難されないか、に重きがあり、ローカルな共同体が弱くなった現代ではマスコミ論調が日本全国の共同体の掟のように感じられ、この規範感が国民に浸透しているのではないか。だから、学校の生徒家庭の緊急連絡網が作れない、といった過剰反応も起こるし、真面目な企業は、レピュテーションリスクという最強の強制力を恐れ、法律上違法ではないと解釈できる範囲であっても萎縮しがちになる。技術の発展に伴い提供できるようになったお客様や社会に役立つサービスを提供することに躊躇する面があり、国際競争という観点からも心配である。本来は、より慎重に検討したわかりやすいスキームを作り、きちんとお客様や社会（とりわけ代表としてのマスコミ）に説明してリスクを低減しつつ、新たなサービスを提供する努力をすれは、マスコミも理解してくれるのかもしれない。もしかしたら、事業者が自らのリスク忌避傾向を棚に上げてマスコミのせいにしている面があるかもしれないが、理解してもらうためにエネルギーがかかることには違いない。

一般に、規範には、法的強制力によるハードローとそれ以外によるソフトローがあるが、日本の個人情報保護規範の状況を図示すると、表 1 のようになる。基本的で基盤となるものから順番に番号を振った。

レピュテーションリスクが規範を動かすことは、決して悪いことではなく、成熟した真面目な社会ということはできる。罰則があるからやるのではなく、社会やお客様の信用のためにやる、というのは、企業の行動としても最も尊敬されるべきことと考える。また、前述のとおり、技術とビジネスの発展のための最小の規制とすることと新しい規範を示すことを両立させるためにできたプライバシーマーク制度は、このような社会の中、良く機能してきた。

---

[11] この事件については、2.2 章に詳説

[12] 2001 年 3 月に提出された当初の法案に対し、マスコミや作家の一部は、取材（個人情報の取得）や公表（第三者提供）が制限され言論の自由を制限するものとして、反対運動を展開。（例えば、2001 年とする「表現の自由を規制する個人情報保護法案に反対する共同アピール」http://www.mediasoken.org/page030.html （2016･11･3）法案修正により、報道機関の報道等が適用除外となった。

[13] 岡村・前掲注 4　31 頁

表 1　規範の種類と強制力

	規範の種類	例	対象	規範レベルの傾向	強制力
8	評判信用	「顧客に誠実な会社」	評判のある者(真面目な事業者)	自由 法律よりかなり高い場合も。 過剰反応誘発	法的強制力はなし。 信用失墜 ﾚﾋﾟｭﾃｰｼｮﾝﾘｽｸ
7	認証マーク	プライバシーマーク	認証受ける者	基準化可能。 法より高いﾚﾍﾞﾙを設定可能	法的強制力はなし。 (取消による信用失墜)
6	(言明)	ﾌﾟﾗｲﾊﾞｼｰﾎﾟﾘｼｰの Web、ﾊﾟﾝﾌへの記載	言明者	自由	(米では言明責任。対すべての人、対顧客) 日:場合によっては欺瞞的商行為？
5	不法行為	漏えい事業者への損害賠償請求	被害者	裁判所による権利侵害・帰責事由・因果関係・損害の判断	提訴した者のみが享受。裁判所の判断による
4	契約	･委託契約の機密保持義務 ･本人特定禁止条項	契約の当事者	基本は自由 (法で義務付けを求めるものもありうる)	法的強制力 （当事者にのみ)
3	(技術)	暗号化	暗号化されたものの使用者	自由	迂回、解読に弱い 法的強制力なし (迂回禁止などの法的手当てがない限り)
2	業界団体ルール	認定個人情報保護団体指針	対象事業者	自由 但し、法の根拠があるときはその枠内。	アウトサイダには効かない。 独禁法とその阻却に注意
1	法律	個人情報保護法	世の中全員	最低限。 理由の例： 社会全員には酷、技術･ﾋﾞｼﾞﾈｽの自由な発達を妨げない	法的強制力 強制力のためには執行が必要

2017 年 8 月現在、15,370 社[14]が認証を受けている。1998 年にスタートした同制度は、個人情報保護の概念や情報セキュリティが社会に根付いていない時期に、それが何なのか、何をすればよいのか、を、企業にわかるように示した。契約文言等に神経質で常に責任を負わないことを志向する企業法務担当にとっては、規格文言の当時の常識とのかい離に戸惑いつつも、その意味するところをかみ砕きつつ、現実的な運用に落とし込んできた。1990 年代から ISO9000 が日本に入ってきてから、製造業を中心としてマネジメントシステムや証跡主義が広がったが、品質は一部の部署が対応すればよかった。しかし、プライバシーマークでは、すべての部署が関係することとなり、良くも悪くも内部統制の先駆けとなった[15]。

このように、日本の社会では、真面目な国民性もあり、評判･信用（８)、認証マーク（７）

[14]一般財団法人日本情報経済社会推進協会(JIPDEC),プライバシーマーク付与事業者一覧 https://privacymark.jp/certification_info/list/clist.html (2017･8･6)

[15] 弊害については、6 章で触れる。

に頼って、個人情報保護規範が定着してきた。考えてみれば、高度情報化社会では、法規制的なハードローだけでなく、認証や自主規制などの強制力のないソフトローによって秩序形成すべき、という考え方からは、この状態は、最も効率の良い強制であり、当然の帰結かもしれない。

しかし、この規範は、「恥」や「非難」は気にしない事業者や、非難されるには小さすぎる事業者には効かない。特に前者に対しては、法的な強制力と機動的な執行力が必要となるが、現実にはそのようには動いていない。2015 年改正前は、個人情報保護法違反は、まず主務大臣が勧告し、命令し、それでも聞かない場合に初めて刑事罰、という間接罰のみが定められており、警察が動くことも難しかった[16]。　後で述べるように、行政の動きも慎重である。2015 年の個人情報保護法改正で、執行力の強化は一部緒についたところ[17]である。消費者が、漏えいした自分の情報が、もしかしたら遵法意識が低く、「恥」も「非難」も気にしない事業者にわたっているのではないか、という不安を抱く背景である。

2.2 個人情報漏えい事故時の損害賠償と保有者の出捐

まず、図 **3** の上流の②個人情報の流出事故を起こした事業者の損害賠償義務や出捐について説明する。

日本では、一旦、大量の個人情報漏えい事故が起きると、情報保有者においては、社会的信用失墜はもちろんのこと、大きな出捐に至る可能性が高い。例えば、①漏えいされた個人からの損害賠償と対応のための弁護士費用、②お詫び金、③記者会見やコンサルタント起用等の費用などがある。このほか、因果関係の立証は難しいかもしれないが、売上の大きな減少といった損害もある。

まず、訴訟による損害賠償である。

個人情報保護法の成立を後押しした宇治市の事件[18]は、エポックメイキングな判例であり、結果的に日本の個人情報漏えい事件における損害賠償判例の方向を決めた。この事件は、住民基本台帳上の市民 22 万人の情報が漏えいした事件である。宇治市が乳幼児健診システムの開発を委託した事業者の再々委託先のアルバイト学生が、データを名簿販売事業者に売却したものである。開発は、初めは宇治市の庁舎内で行われていたが、システムへのデータの落し込み作業においてエラーが頻発したため、作業が終わらず、B 社は宇治市担当職員の口頭での承諾を得て、データを光磁気ディスクにコピーして持ち帰り、再委託先の社屋で作業を行っていた。ところがアルバイト学生はそのデータを自分のコンピュータのハードディスクにコピーし、名簿販売事業者に 258,000 円で売却した。それが流通して結婚相談事業者や成人式用着物販売事業者から適齢期の家庭にダイレクトメールが送付され発覚した。

1999 年 5 月頃、新聞紙上で、本件データが外部に流出し名簿販売業者がインターネットの

---

[16] 個人情報保護法起草時、真面目な民間企業は、米国的なソフトローによる秩序作りを支持していただけでなく、当時のビジネス慣行に照らしても慣れない規律でもあり、いきなり取締られるのは困る、との立場で意見表明しており、間接罰になったこと自体は問題はない。

[17] 40 条で、個人情報保護委員会の立入調査権が定められた。直罰は、83 条の、事業者やその役員、（元）従業員が、自己若しくは第三者の不正な利益を図る目的で個人情報データベース等を提供・盗用した場合に限られている。

[18]大阪高判平 13・12・25 判例地方自治 265 号 11 頁、最 1 小判平 14・7・11 判例地方自治 265 号 10 頁

ホームページでその購入を勧誘する広告を掲載している、との記事が大きく報道され、社会的に問題となった。

宇治市は、すぐに事実を確認し、名簿販売事業者からディスクを回収し、コンピュータのデータも削除してもらった。更に、記者会見や市政だより等によって、市民に対し事実を説明し、道義的な意味で謝罪し、各種の再発防止策を講ずることとした。

損害賠償については、個人情報が漏えいした市民 3 名が提訴したものである。裁判所は、基本 4 情報は、社会生活上、本人と関わりのある一定の範囲のものには既に了知され、利用され得る情報ではあるが、本件データには、転入日、世帯主、世帯主との続柄など一般には知られていない情報も含み、世帯ごとに関連付けられ整理された一体としてのデータであることから、明らかに私生活上の事柄を含むものであり、一般通常人の感受性を基準にしても公開を欲しないであろう考えられ、さらには未だ一般の人に知られていない事柄と言える、として、プライバシー侵害を認めた。当時、住民基本台帳は、自由に閲覧でき、コピーも入手できたが、判決は、閲覧や交付請求には、氏名、住所、請求事由を明らかにするなど、一定の手続きの制約を課せられており、不当な目的に使用される恐れがあるときは市町村長が閲覧や交付の請求を拒否できることから、プライバシー侵害を否定するものではないとしている。被害については、現に商品の勧誘を受ける等を具体的被害と言及している。

アルバイト学生の故意の不法行為に対する宇治市の民法 715 条に基づく使用者責任については、再委託の承認、再々委託先の関係者との打ち合わせにアルバイト学生も参加していたこと、アルバイト学生は当初宇治市の庁舎内で開発していたこと、だから、データの持出の承諾を求めたことから、宇治市とアルバイト学生の間に実質的な指揮・監督関係を認めている。

そして、一人当たり、1 万円の慰謝料と 5000 円の弁護士費用を認めた。

その後も、ヤフーBB 個人情報漏えい事件[19]では漏えい 660 万人中 5 名が提訴している。

この事件は、インターネット接続サービスプロバイダのヤフーBB が、顧客データを含むデータベースサーバのリモートメンテナンスサーバから、元派遣社員がインターネットを通じて顧客データをダウンロードし、共犯者に渡したものである。

元派遣社員がリモートメンテナンス用のサーバにアクセスできる権限はあったが、ID はグループで共有していた。また、個別のユーザも管理が甘く、ユーザ名とパスワードが同じものが多数存在しており、定期的な変更もなかった。元派遣社員は、外部からアクセスする権限はなかったが、派遣中にアクセスしていたバックアップサーバなどに保存されていたアカウント情報を使って、派遣終了後、外部から侵入し、退職後、パスワード変更もされていないグループ ID でメンテナンス用のデータをダウンロードした。

共犯者からデータを転得した者が、ヤフーBB を恐喝したことから、事件が発覚した。

事件発生時は、個人情報保護法は成立していたものの、まだ施行されていなかった[20]ことから、判決は、インターネット接続サービス事業者は、電気通信事業法上の電気通信事業者であり、不正行為が行われた当時、電気通信事業における個人情報保護に関するガイドライン（平成 10 年 12 月 2 日郵政省告示 570 号）5 条 4 項は、「電気通信事業者が個人情報を管理

[19]大阪地判平 18･5･19 判時 1948 号 122 頁

[20] 2003 年 5 月 30 日成立、2005 年 4 月 1 日全面施行

するに当たっては、当該情報への不正なアクセス又は当該情報の紛失、破壊、改ざん、漏えいの防止その他の個人情報の適切な管理のために執拗な措置を講ずるものとする。」と定めていたことを挙げ、アカウント管理の杜撰さから過失を認定した。

権利侵害性については、流出した個人情報は、①住所②氏名③電話番号④メールアドレス⑤ヤフーＩＤ⑥ヤフーメールアドレス⑦申込日で、①～⑥は個人の識別等を行うための基礎的な情報であって、その限りにおいて秘匿されるべき必要性が高いものではなく、本件サービスの会員であるということやその申込日についても同様、としながらも、このようなものでも本人が、自己が欲しない他者にはみだりにこれを開示されたくないと考えることは自然であり、そのことへの期待は保護されるべき、として、プライバシーに係る情報としての法的保護の対象となる、と判断している。

損害については、原告は、不特定の第三者にいついかなる目的で個人情報が利用されるかわからない不安感を主張したが、裁判所は、確かに恐喝を行うような者の手に渡ったことからそれらの者が自己の利益を図るために利用する危険性はあったが、既に回収済みで二次流出があったと認められない状況であり、不安感はさほど大きくない、と判示している。

結局、元々秘匿性が高くないこと、ヤフーがすぐに発表を行い、不正取得された顧客に連絡するとともに、500 円の金券を交付するなどして謝罪を行う一方、セキュリティ強化を図っていることから、慰謝料は一人当たり 5000 円とされた。

TBC 顧客情報漏えい事件[21]では、エステティックサロンを展開する TBC グループから、Web サイトで実施したアンケートのデータや，資料請求のために入力されたデータなど，およそ 5 万人分のデータが外部から閲覧できる状態になっており、複数の者がダウンロードすることで流出したケースである。原因は、2002 年 3 月末から 4 月上旬にかけてサーバの移設を行った際、委託先が、約 5 万人分の個人情報を含む電子ファイルを Web サーバの公開領域に置きながら，アクセス制限の設定をしなかったことである。事件が発覚したのは個人情報保護法成立前の 2002 年 5 月 26 日で、その日のうちにサーバ上から削除されたが，アンケートへの回答など身体的特徴といったセンシティブ情報が含まれており、流出後には、ファイル交換ソフト上などで流通し、いたずら電話やダイレクトメール、ウイルスの送付といった二次被害が拡大した。

個人情報流出によりプライバシーを侵害されたとして被害者 14 人が 1 人当たり 115 万円の損害賠償を求めたが、東京地方裁判所は、原告 13 名に 1 人当たり 3 万 5000 円（慰謝料 3 万円，弁護士費用 5000 円），1 名に 2 万 2000 円（慰謝料 1 万 7000 円，弁護士費用 5000 円）の賠償金を支払うように命じた。

その後、2014 年に発生した大量漏えい事件まで、大きく報道される民事訴訟はない。

2013 年成立した「消費者の財産的被害の集団的な回復のための民事の裁判手続の特例に関する法律」で創設された消費者団体訴訟制度では「精神上の苦痛を受けたことによる損害」は対象外である。しかし、2014 年に発生した大規模な個人情報漏えい事件では、弁護士が web や記者会見で原告を募り、原告数を単純合計すると、1 万名規模の訴訟となっている[22]。この

[21]東京高判平 19･8･28 判タ 1264 号 299 頁
[22]例えば、http://www.benesse-saiban.com/pc/index.html　（2017･2･7）

流れからは、今後の漏えい事故が起きた場合には同様の原告数の規模となると考えられ、損害賠償額合計はかなり高額になる可能性がある。

また、日本では、しばしば漏えいの通知と共に、「お詫びの印」として、500 円～1000 円程度の商品券などが提供されている[23]。これは、2002 年 56 万人の情報漏えいを起こしたローソンが 500 円の商品券を 115 万人に送付したことに倣ったものだが、しばしば損害賠償と誤解されることがある。但し、三菱 UFJ 証券で内部犯行により職業・年収区分・勤務先・部署・役職・業種等を含む顧客情報が名簿販売事業者に売られた事件では、流出した約 5 万人に対して、1 万円相当のギフト券が贈られたが[24]、このケースは自主的賠償とみることもできる。

2.3 日本における名簿販売事業者の実態

不適正な流通として、すぐに念頭に浮かぶのは、名簿販売事業者である。個人情報保護法が施行された 2005 年以前は、プライバシー上の懸念はあったものの、名簿販売事業者は必ずしも違法な事業ではなかった。2006 年住民基本台帳法が改正されるまでは、住民基本台帳でさえ公開で、閲覧、書き写しは可能であった。2015 年改正前の個人情報保護法では、取得に関しては、17 条で、「偽りその他不正の手段により個人情報を取得してはならない」と抽象的な適正取得の規定があるだけであり、提供に関しては、23 条 2 項に基づき、オプトアウト手続きによる第三者提供が可能である。オプトアウト手続きは、個人情報保護法成立時に、住宅地図や電話帳のビジネスを念頭に、予め第三者提供することと項目、方法、本人が要請すれば提供を止めることを、本人通知又は公表することで、事前に同意なく第三者提供することができるとしたものである。

2016 年 3 月、消費者庁は「名簿販売事業者における個人情報の提供等に関する実態調査報告書」を公表した。名簿販売事業者 8 社にヒアリングをした内容で、官庁のヒアリングに応じているところから、名簿販売事業者の中では、比較的まじめな者と思われるが、実態を垣間見ることができる。

主な入手先や提供先など、流通の概要は図 **4**[25]のとおりである。

---

[23] お詫び金については、菅原尚志　原田要之助、「企業・組織における個人情報漏えい事故の補償について―お詫び金に着目した考察―」、情報処理学会研究報告　2013 年 5 月 16 日、及び、みずほ中央法律事務所の Web サイトが詳しい。
http://www.mc-law.jp/kigyohomu/9055/　(2017･2･5)
また、分析として、田中智大、原田要之助「個人情報漏えいに対する補償についての考察―お詫び金と賠償金―」2015 年 11 月 20 日 lab.iisec.ac.jp/~harada_lab/lab/2015/IPSJ-EIP15070004.pdf　(2017･1･28)

[24] 「顧客情報流出による損失 70 億円超と試算、三菱 UFJ 証券」,ITPRO(2009 年 9 月 9 日)
http://itpro.nikkeibp.co.jp/article/NEWS/20090909/336929/?rt=nocnt　(2017･3･30)

[25] 消費者庁『名簿販売事業者における個人情報の提供等に関する実態調査　報告書』11 頁図（2016 年 3 月）

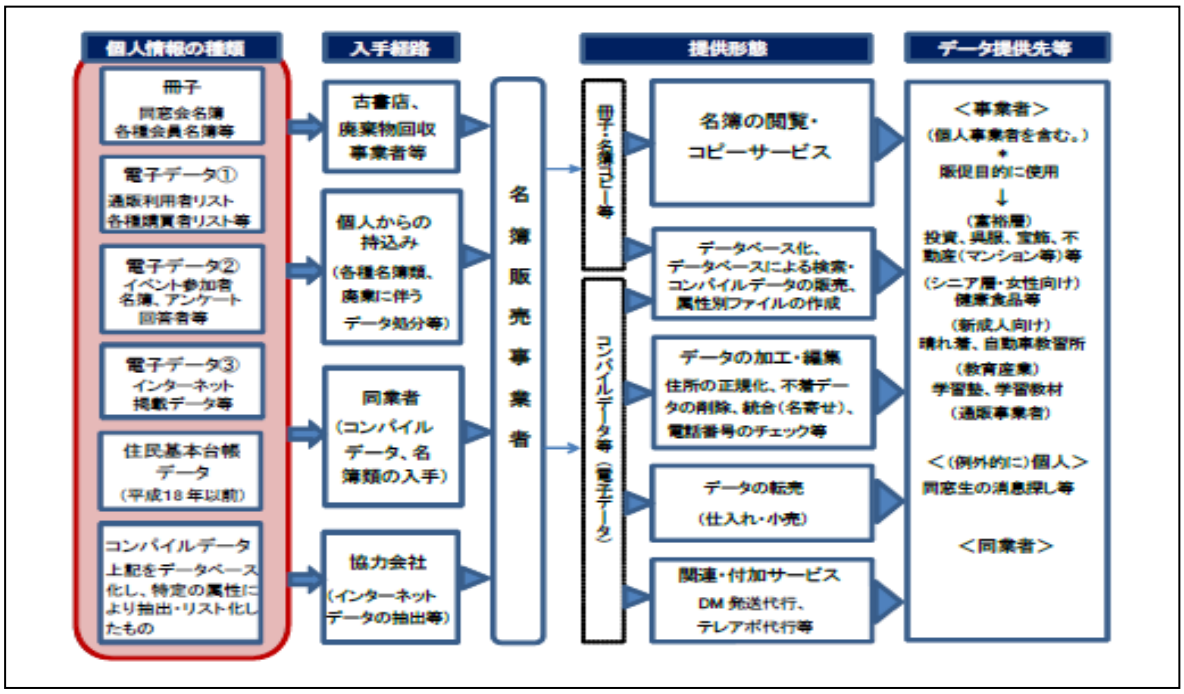


図 4　名簿販売事業者の入手先と販売先

取得に当たっては、個人からの取得は身元確認のため運転免許証のコピーなどを提供させる者もいる。入手経路については特に確認をしないが、問題がないことの「確認書」を出させている者もある。売り手がメールで「問題がないデータ」と記載していることを根拠に購入する例もある。

オプトアウト手続きについては、4 社は第三者提供を利用目的としているが、法の定める記載事項を記載せず、3 社については、第三者提供を利用目的とすることさえ記載していなかった。つまり、現行法でも違法な事業者ということになる。

本人から要請があれば、本人確認の上、データベースから消去しているといい、名簿を提供した先の事業者にも削除するように依頼しているという。名簿販売事業者の団体である NPO 法人「日本個人データ保護協会」では、本人からの第三者提供停止の要請があれば、加盟会員で共有する仕組みがあるという。一部のアウトサイダの存在が自分たちのようなコンプライアンスを心がけている事業者のビジネスの障害となっている、解決策として登録制にして、何らかの報告・監査制度を導入し、正々堂々と事業ができる環境ができることが望ましい、と、ヒアリングに応じた複数の事業者は主張している。

このように、本人関与には対処するが、取得時の適正性の確認には敢えて深く聞かずに売買していることが不正な流通の温床となっている。このヒアリングに応じた者よりも悪質な名簿販売事業者には、騙されやすい消費者のリスト（いわゆる「カモリスト」）を取引し、犯罪に詐欺等の犯罪行為に加担し、不適切な勧誘等による消費者被害を助長する者もおり、社会問題として指摘されていた。2014 年、2015 年個人情報保護法改正の実質的な大綱である「パーソナルデータの利活用に関する制度改正大綱[26]」が出されたが、その中でも「いわゆる名簿

[26] 高度情報通信ネットワーク社会推進戦略本部「パーソナルデータの利活用に関する制度改正大綱」2014 年 6 月

屋」問題は、社会問題として継続検討、とされていた[27]。

2.4 2016 年までの個人情報保護法の執行状況

2.4.1 個人情報保護法上の実効性担保の枠組み

2016 年までの個人情報保護法の執行状況を見る前に、まず、この時期適用されていた 2015 年改正前の個人情報保護法が用意した実効性の担保の枠組みを説明する。2.4 節で用いる条文は、すべて改正前のものである。

個人情報保護法は、その実効性の担保として、強制力のない苦情処理と、行政処分としての主務大臣による関与を定めている。

2.4.1.1 苦情処理

個人情報保護法制定以前から、民間部門では自主的な取り組みにゆだねられてきたが、そこでは、事業者が不適切な取扱いを行ったときは、本人から当該事業者や事業者団体に対して苦情が申し立てられ、それによって解決が図られてきた。[28]このように、トラブル解決の迅速性と経済性から、訴訟等によるよりも、むしろ苦情処理制度による解決が適当なものが多い。そこで、改正前個人情報保護法では、

①個人情報取扱事業者による苦情処理
②認定個人情報保護団体による苦情処理
③国・地方公共団体による苦情処理

の仕組みを定めている。これらは並列であり、①を経ないと②や③に進めない、というものではない。

まず、31 条で、個人情報保護取扱事業者自身が、個人情報の取扱いに関する苦情の適切かつ迅速な処理に努めなければならない、としている。そして、第 2 項では、その目的を達成するために必要な体制の整備に努めなければならない、としている。

それぞれ、努力義務なので、違反しても、主務大臣の報告聴取や助言の対象となるが、勧告、命令の対象ではない。しかし、個人情報の中でも、保有個人データについては、法 24 条 1 項 4 号と施行令 5 条 1 項で、その事業者が行う保有個人データの取扱いに関する苦情の申出先の公表等が義務付けられており、その違反については勧告や命令の対象となる。

苦情は、義務規定の違反に限らず、個人情報の取扱に関するものであれば足りる。苦情の対象となる個人情報は第三者のものでもよい[29]。

必要な体制とは、基本方針によれば、苦情受付窓口の設置、苦情処理手順の策定等としている。

次に認定個人情報保護団体による苦情処理である。全国にある多種多様な事業者に関する

---

24 日
[27] 同・Ⅶ継続的な検討課題　4　いわゆる名簿屋
[28] 岡村・前掲注 4　303 頁
[29] 岡村・前掲注 4　305 頁

苦情を国がすべて見ることは現実的ではない。個人情報保護法成立前には、個人情報の保護が重要な、通信、金融、健康の分野で省庁が指針を出し、事業者団体にガイドラインを策定させ、関係事業者が自主的に遵守してきたこともあり、このような取り組みを尊重・支援する仕組みとして、認定個人情報保護団体として国が認定し法律上の制度とした。ある意味、主務大臣制から連想される行政指導の枠組みに似ている。本人等は、認定個人情報保護団体に苦情を申し立てることができ、認定個人情報保護団体は、本人に必要な助言をし、その苦情にかかる事情を調査し、当該事業者に対し、その苦情の内容を通知してその迅速な解決を求めなければならない。また、必要があるときは、対象事業者に対し、文書・口頭による説明を求め、資料の提出を求めることができ、対象事業者は正当な理由なく拒んではならない。

そして、国や地方公共団体による苦情処理である。法 9 条は、「国は、個人情報の取扱いに関し事業者と本人との間に生じた苦情の適切かつ迅速な処理を図るために必要な措置を講ずるものとする。」と定め、13 条は「地方公共団体は、個人情報の取扱いに関し事業者と本人との間に生じた苦情が適切かつ迅速に処理されるようにするため、苦情の処理のあっせんその他必要な措置を講ずるよう努めなければならない。」とした。

「あっせん」とは、苦情を当該事業者、認定個人情報保護団体、主務大臣等へ情報提供することで当該情報の関係者間での解決を促すことをいい、「その他の必要な措置」とは、助言、指導を含む[30]。個人情報に関する苦情の大部分が事業者が消費者の個人情報を利用した結果として起こる消費生活上の苦情であり、相談者の立場として、消費生活に関する苦情から個人情報の問題だけを取り出して相談することは難しく不便なことから、基本方針では、「地方公共団体における取組のあり方」として、既存の消費生活センターや消費者相談窓口を個人情報に関する苦情の窓口とする、としている。そして、事業者側を監督支援するような、各事業・事業者の振興・支援を担う部局等の関係部局と、実効のある連携を確保する仕組みが、相談者の利便性等の観点から望まれるとしている。

2.4.1.2 主務大臣の関与

2015 年改正前の個人情報保護法は、強制力のある枠組みとして、主務大臣制を取っていた。

欧州では、特定の省庁とは独立した統一的な第三者機関にゆだねており、そのような意見もあったが、法成立前から業界別に監督官庁の指針の下に事業者団体が運営していたことから、継続して主務大臣を監督機関としての地位に置いた。制定時としては、個人情報保護法は、それまでの慣習より踏み込んだ細かな内容であり、些細なことで罰則に触れることを恐れた事業者にも納得性はあった。

主務大臣は、法 36 条で定めており、雇用管理については厚生労働大臣、それ以外は事業者の事業を所管する大臣である。但し、内閣総理大臣は、円滑な実施のため必要がある場合は、個人情報取扱事業者が行う個人情報の取扱いのうち特定のものについて特定の大臣又は国家公安委員会を主務大臣に指定することができる、としている。そして、政府の基本方針では「所管が明らかでない場合」には、内閣府は、各省庁の所掌事務に照らして関係の深い省庁に照会の上特定し、又は関係省庁連絡会議を活用することにより、指定を行うこととさ

[30] 岡村・前掲注 4　308 頁

れている。

監督の内容は、報告聴取、助言、勧告、命令、である。

主務大臣は、個人情報取扱事業者の義務等の施行に必要な限度において、個人情報取扱事業者に対し、個人情報の取扱に関し、報告聴取（32 条）を行うことができ、また、助言（33 条）をすることができる。この報告聴取は、後述する侵害通知における監督官庁への報告のような義務のない自主的なものや、相談に応じた簡単な助言とは違い、行政処分としての報告聴取や助言である。従って、行政不服審判法に基づき不服申立てや行政事件訴訟法に基づき取消しを求めることができる。また、「施行に必要な限度」なので、些細な問題は対象ではない。

主務大臣は、法 34 条 1 項に基づき、事業者が義務規定に違反した場合において個人の権利利益を保護するため必要があると認めるときは、当該違反行為の中止その他違反を是正するために必要な措置をとるべき旨を勧告することができる。勧告の制度は、本来は、報告聴取・助言では自主的な問題解決が図られないときのために、より強い行政の直接関与による最終的な是正手段として、命令の制度（同条 2 項・3 項）とともに置かれている[31]。勧告を行うためには、単に違反行為が存在するだけでは足りず、「個人の権利利益を保護するために必要があると認めたとき」としているのは、違反状態の放置により、個人の権利利益を侵害する恐れが高く、義務を履行させることを要すると、主務大臣が客観的合理的見地から判断した場合をいう、とされている。[32]

そして、勧告を受けた個人情報取扱事業者が正当な理由がなくてその勧告に係る措置をとらなかった場合において個人の重大な権利利益の侵害が切迫していると認めるときは、主務大臣は命令することができる。そして、それに応じなければ、初めて罰則が適用される。（法 74 条）

2.4.2 施行状況

法 69 条は、個人情報保護法の施行状況を取りまとめて国会に対し報告し、概要を公表することを求めている。これに基づき公表された「平成 26 年個人情報の保護に関する法律　施行状況の概要」による施行状況は以下の通りである。

まず、国・地方公共団体が行う苦情処理について。

2015 年には、地方公共団体と国民生活センターが受け付けた苦情は 6,009 件だった。その内容別の状況を表 2 に示す。「不適正な取得」については 2,539 件と全体の 42.3%を占めている[33]。おそらく提供したつもりがないのになぜ持っているのか、という内容と思われる。

---

[31] 岡村・前掲注 4　317 頁（園部編 200 頁を引用）

[32] 岡村・前掲注 4　318 頁（園部編 202 頁を引用）

[33] 個人情報保護委員会『平成 27 年度 個人情報の保護に関する法律 施行状況の概要』8 頁（2016 年 10 月）http://www.ppc.go.jp/files/pdf/personal_sekougaiyou_27ppc.pdf　(2017.6).

表 2 苦情相談内容の状況

苦情相談内容	2015 年		2014 年度	
	件数	(割合)	件数	(割合)
不適正な取得	2,539	42.3%	3,089	43.5%
漏えい・紛失	1,450	24.1%	1,950	27.5%
同意のない提供	1,022	17.0%	1,172	16.5%
目的外利用	619	10.3%	781	11.0%
開示等	163	2.7%	200	2.8%
苦情等の窓口対応	188	3.1%	244	3.4%
情報内容の誤り	58	1.0%	95	1.3%
オプトアウト違反	20	0.3%	58	0.8%
委託先等の監督	24	0.4%	41	0.6%
その他	1,189	19.8%	1,169	16.5%
合計（重複分を除く）	6,009	100%	7,101	100%

そして、その処理結果は表 3 のとおりである。
主務大臣や警察などへの他機関紹介は 2.2%となっており、ほとんどは自主解決かあっせん解決となっている。

表 3　苦情処理結果の状況

苦情相談内容	2015 年		2014 年度	
	件数	(割合)	件数	(割合)
助言（自主交渉）	4,751	79.1%	5,677	79.9%
その他情報提供	800	13.3%	969	13.6%
あっせん解決	147	2.4%	156	2.2%
他機関紹介	133	2.2%	125	1.8%
処理不要	86	1.4%	110	1.5%
処理不能	31	0.5%	38	0.5%
あっせん不調	7	0.1%	8	0.1%
未入力(処理中)	54	0.9%	18	0.3%
合計	6,009	100%	7,101	100.0%

次に、主務大臣の権限行使は、図 **5** のとおりである。

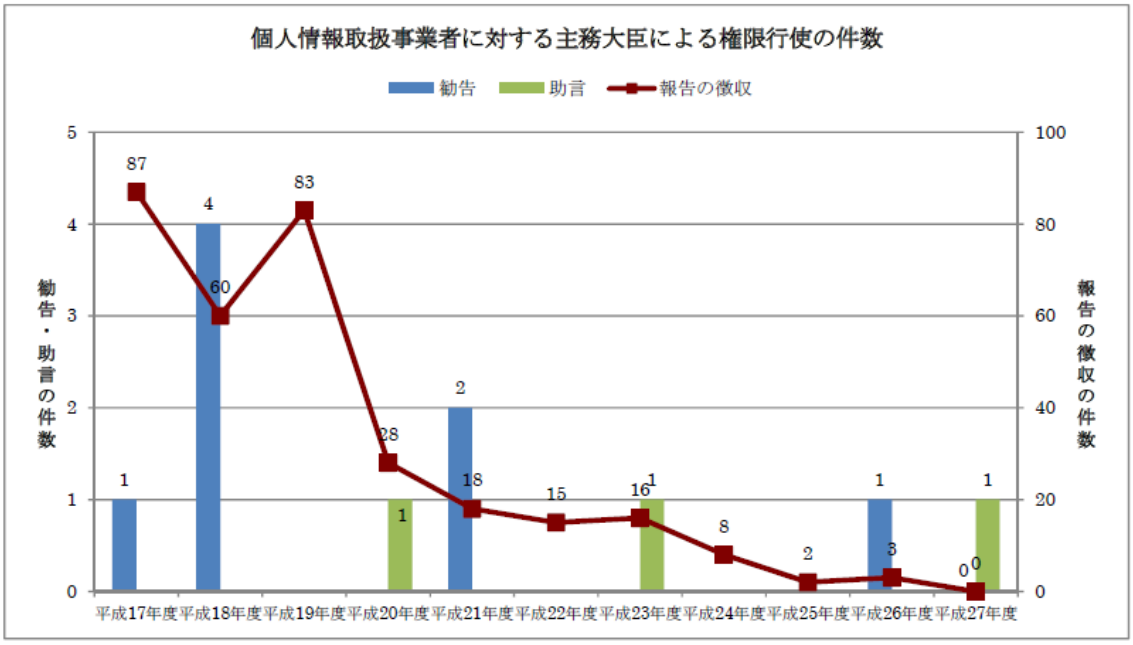


図 5　主務大臣権限行使件数

後述する侵害通知として、ガイドライン[34]に基づく自主的で非公式な報告は行われていたとは推測されるが、法第 32 条に基づく公式な報告聴取件数は 2008 年くらいから激減し、改善勧告の数も少ない。

報告聴取の官庁別推移[35]は、図 6　のとおりである。圧倒的に金融庁が多く、次が大きく離れて経産省である。金融機関に対する検査等で、対象事業者へのグリップも効いており、実態も把握できるためとも思われる。

[34] この図の時点で有効だったものとして、『個人情報の保護に関する法律についての経済産業分野を対象とするガイドライン』(平成２１年１０月９日厚生労働省・経済産業省告示第２号）28 頁

[35] 図 6 図 7 は、各年度の個人情報保護法を担当する官庁による「個人情報の保護に関する法律 施行状況の概要』から作成

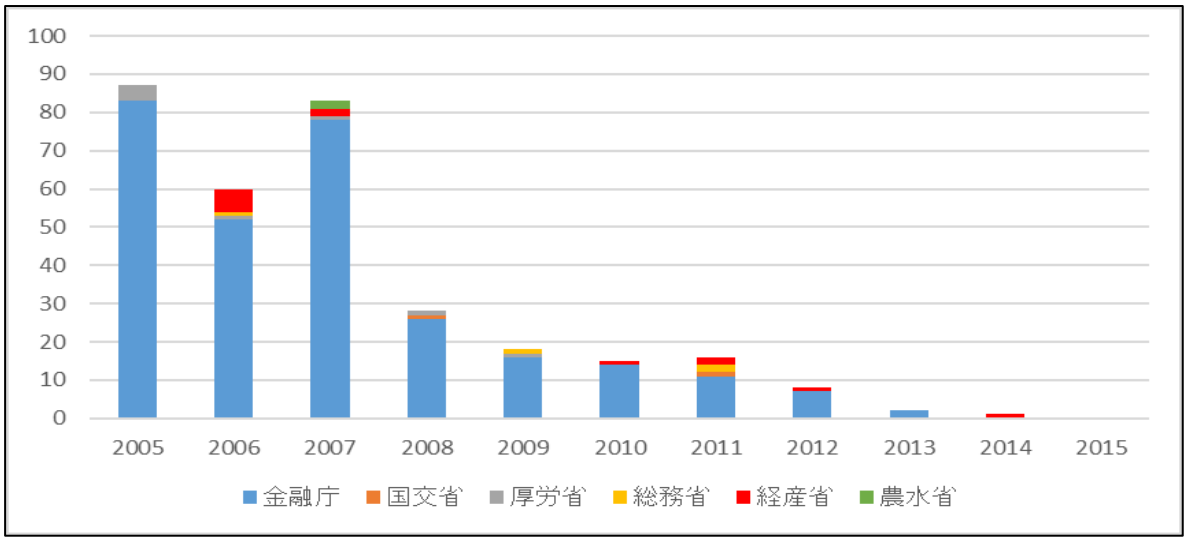


図 6　報告聴取の官庁別推移

また、報告聴取の違反容疑別推移は、図 7 のとおりである。

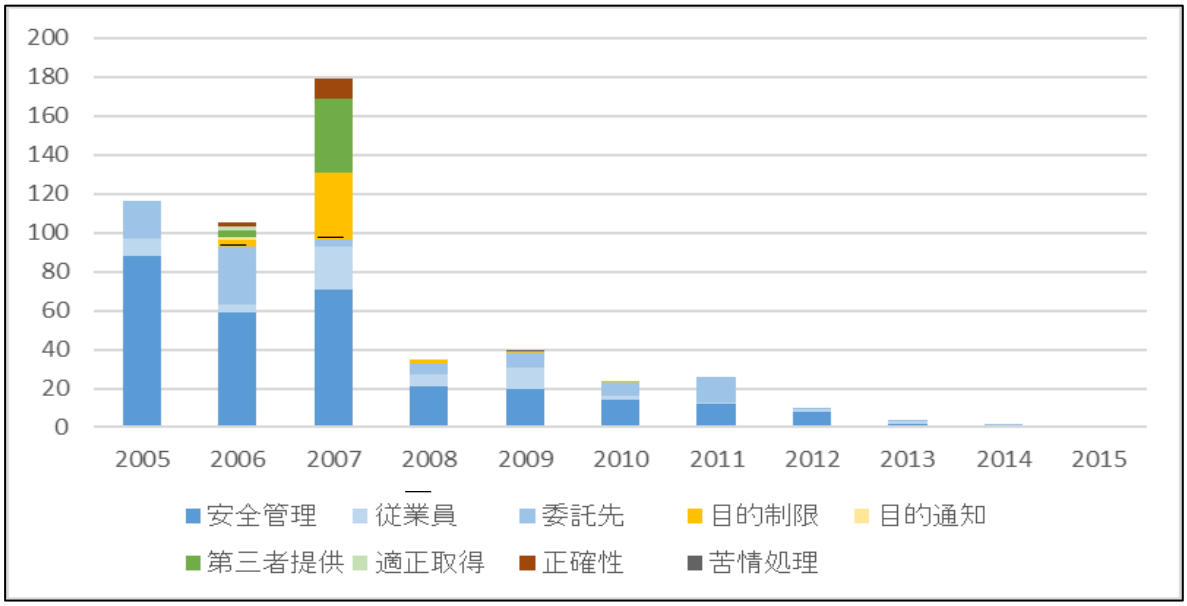


図 7　報告聴取の違反容疑別推移

安全管理、従業員管理、委託先管理の、安全管理系が圧倒的に多いが、初期のころは、目的外利用や、第三者提供・不適正取得もあった。

次に助言についてである。2015 年のものを除き、助言については、概要も開示されていないが、2008 年は財務省、2011 年は経産省が出したものだが、それぞれ、安全管理（従業員管理、委託先管理含む）に関するものである。

最後に改善勧告についてである。2015 年度までに出された勧告 8 件は表 **4** のとおりである。2015 年度までに出された勧告 8 件はすべて安全管理措置違反で、そのうち 6 件は、事業

者が自主的に報告したか公表した事案に対し正式な報告聴取を行い勧告を出したものである。

表 4　概要が開示されている処分事案

年	官庁	種類	分野		契機
2005	金融庁	勧告	安全管理、従業員の監督	みちのく銀行	事業者からの報告
2006	金融庁	勧告	安全管理、従業者の監督	株式会社みずほ銀行	事業者からの報告
2006	総務省	勧告	安全管理、従業者の監督	KDDI 株式会社	事業者からの報告
2006	経産省	勧告	欄外※１	株式会社ソニーファイナンスインターナショナル	個人から官庁への情報提供※２
2006	経産省	勧告	欄外※１	ＵＦＪニコス株式会社（現三菱ＵＦＪニコス株式会社）	個人から官庁への情報提供※２
2009	金融庁	勧告	安全管理　従業員管理	三菱ＵＦＪ証券	事業者が漏えい事実を公表
2009	金融庁	勧告	安全管理、委託先監督	アリコジャパン	内部調査結果の最終報告を受けて
2014	経産省	勧告	安全管理、委託先監督	株式会社ベネッセコーポレーション	事業者からの報告＋報告徴収
2015	厚労省	助言	安全管理、従業員監督	株式会社クリエイトエス・ディー	事業者が相談

※１　利用目的制限、適正な取得、取得に際しての利用目的通知、安全管理措置、従業者の監督
※２　ある個人から経済産業省に対し、個人信用情報機関から入手した個人信用情報を販売している業者に関する情報提供があったことを受けて

このほか、2011 年 5 月 1 日には、株式会社ソニー・コンピュータエンタテイメントに対し、世界的なハッキングによりプレイステーションネットワーク（PSN）に登録した氏名、住所、電子メールアドレス、生年月日、パスワードと PSN の ID が漏えいした事案について、個情法 32 条に基づく報告聴取を行い、同月 27 日、「個人情報保護法 33 条に基づく指導[36]」を行っている。2015 年改正前は、法 33 条は「助言」しか定めておらず、「指導」を行ったことには疑問がある[37]。

[36] 経産省「株式会社ソニー・コンピュータエンタテイメントに対する個人情報保護法に基づく指導について」（2011 年 5 月 27 日）
[37]大島義則他、『消費者行政法』290 頁（勁草書房、2016）　なお、施行状況の概要には、報告聴取案件として扱

2.4.3 分析

この状況を、1.3 節で示した上流、中流、下流について分析する。

まず、主務大臣による強制力のある処分について分析する。

報告聴取については、2007 年がピークであり、2008 年から件数が激減している。これは、2007 年、個人情報保護法への過剰反応が問題となり、政府の執行方針も変化したためと思われる[38]。個人情報保護法は、基本方針において、全面施行後 3 年を目途として検討を加えることになっており、2007 年、国民生活審議会において検討を進め、2007 年 6 月 29 日には、「個人情報保護に関する取りまとめ」[39]を政府に提出した。その中の一項目に、過剰反応への対応があった。翌 2008 年 4 月 25 日、個人情報の保護に関する基本方針が改定され、「いわゆる『過剰反応』を踏まえた取組」として 1 節が割かれ、国や地方公共団体の啓発義務が定められた[40]。同方針の国が講ずべき個人情報の保護のための措置に関する事項では特に執行方針を弱めてはおらず、むしろ悪質な事業者の監督の強化を求めている[41]が、過剰反応への何らかの配慮があったのかもしれない。

報告聴取の対象とした違反容疑は、大半は安全管理義務違反容疑である。これは、2.1 節で説明した個人情報保護法の成り立ちの影響もあろう。基本方針でも、「２（２）政府全体としての制度の統一的な運用を図るための指針　①個別の事案が生じた場合の内閣府と各省庁の連携」において、「大規模な個人情報の漏えい等の個別の事案が発生した場合」とあり、事案の代表例が漏えい事故と捉えられている。

安全管理義務は、本質的に対象が上流の事業者であり、そこがターゲットとなる。初期のころは、第三者提供や目的外利用、不適正取得など、中流、下流の事業者を対象としたと思われる報告聴取が少ないながら行われているが、2008 年以降は全くない。

助言も、改善勧告も、安全管理が対象であり、上流の①取得事業者に対してである。

強制力につながる主務大臣の勧告は、8 件しか出ておらず、漏えい事故の数から考えると、かなり重要なケースに限られているようではある。しかし、前述のとおり、8 件のうち 6 件は、事業者が自主的に報告したか公表した事案に対し、行政処分としての報告聴取を行い、勧告を出したものである。自ら報告するような事業者は当然再発防止策も計画しているはずで、個別のケースにおいては 2.4.1.2 節で説明した勧告の趣旨にいう、「違反状態の放置により、個人の権利利益を侵害する恐れが高く、義務を履行させることを要すると、主務大臣が

われている。消費者庁『平成 23 年度 個人情報の保護に関する法律 施行状況の概要』36 頁（2012 年 9 月）

[38] 過剰反応への対応については、消費者庁『平成 19 年度 個人情報の保護に関する法律 施行状況の概要』4 頁（2008 年 9 月）

[39] 審議会の意見書における必要な措置の内容（概要）
① いわゆる「過剰反応」に対応した広報啓発
② 各省庁ガイドラインの共通化について必要な検討
③ 事業者の自主的な取組の促進（基本方針の見直し等）
④ 市販の名簿の管理方法の検討（基本方針の見直し等又は政令改正）
⑤ 国の行政機関における必要な行政運営上の改善
⑥ 防災等の地方の取組について、各施策の担当省庁で必要な検討

[40] 『個人情報の保護に関する基本方針』1 (2)②　2008 年 4 月 25 日

[41] 同　2 (3)①では、「また、また、悪質な事業者の監督のため、個人情報取扱事業者に対する報告の徴収等の主務大臣の権限等について、これを適切に行使するなど、法等の厳格な適用を図るものとする。」としている。

客観的合理的見地から判断した場合」とは考えられないが、恐らく、1.2.1 節で述べた、世の中に指針を示す、という位置づけと思われる。確かに、初期のころは、有名な会社が改善勧告まで出された、という報道に接し、一般の事業者も安全対策の重要性を認識し、対策を強化した。そういう意味では、法的な評価は別として、社会に対する実効性の確保なのだろう。

次に、地方公共団体の消費者センターや国民生活センターが受け付けた苦情相談である。前述のとおり、苦情の 42.3%が不正な取得に関するものである。おそらく提供したつもりがないのになぜ持っているのか、という内容と思われ、下流事業者、つまり、買取った個人情報を利用する事業者に関するものと考えられる。

これを調査すれば、その上流の名簿業者にも行きつくはずだが、なぜ、これが強制力のある調査に至っていないのだろうか？

消費者センターは、前述のとおり、地方公共団体の苦情処理の役割を実行している。地方公共団体は、法 67 条及び施行令 11 条 1 項により、主務大臣の執行権限の事務を処理することができる。しかし、それは行われていないようである。国民生活センターも自ら苦情相談に取組むが、あっせんなので、目の前の消費者の救済に力を注ぎ[42]、消費者センターも同様と考えられる。相談内容は「全国消費生活情報ネットワーク・システム」（PIO-NET）に蓄積され、各省庁もアクセスして閲覧・検索することができる。1984 年に開始され、2016 年 5 月現在、累計約 1992 万件が登録されている。PIO-NET の目的の一つは、行政機関による消費者被害の未然防止・拡大防止のための法執行への活用であり、各省庁は、法令の執行又は消費者政策の立案等のために必要な限度で利用することになっている。各省庁には、基本方針に基づき、窓口となる職員は明確になっているが、兼務も多く、積極的にデータベースから事案を探す体制にはなっていなかった。

特に、名簿販売事業者に関しては、主務大臣制の中で、主管する大臣が決まっていなかったため、どの官庁も当事者意識は持っていなかった。2007 年初頭に明らかになった個人情報の大量漏えいと漏えいした情報を使った詐欺事件[43]を受け、前述[44]のとおり、2007 年 6 月 29 日付の国民生活審議会の「個人情報保護に関する取りまとめ」には、必要な措置の一つとして、「市販の名簿の管理方法の検討（基本方針の見直し等又は政令改正）」が取り上げられた。これを受けた 2008 年 4 月 25 日付の個人情報の保護に関する基本方針改正においては、前文で「実際、事業者からの顧客情報等の大規模な流出や、個人情報の売買事件が多発し、社会問題化している。それに伴い、国民のプライバシーに関する不安も高まっており、また、安全管理をはじめとする企業の個人情報保護の取組への要請も高まっている。」とし、「個人情報取扱事業者に関する事項」と、「国が講ずべき個人情報の保護のための措置に関する事項」に改定があった。

「６．（１）個人情報取扱事業者に関する事項」では、「②消費者等の権利利益の一層の保護」の一つとして、「事業者の個人情報保護を推進する上での考え方や方針には、消費者等、本人の権利利益保護の観点から、以下に掲げる点を考慮した記述を盛り込み、本人からの求

---

42 国民生活センターの国への移行を踏まえた消費者行政の体制の在り方に関する検討会　第 8 回検討会資料２－３『国民生活センターにおける相談（あっせん）』9 頁

43 2007 年 2 月 20 日及び 3 月 12 日、大日本印刷は、クレジットカード会社から受託した個人情報約 863 万件が委託先社員により持出され、インターネット通販詐欺グループに売り渡され、49 会員、667 万 2,989 円の被害が出たことを公表した。

44 前掲注 39

めに一層対応していくことも重要である。・・(中略)・個人情報の取得元又はその取得方法（取得源の種類等）を、可能な限り具体的に明記すること。」と定めた[45]。しかし、具体的な推進はなかった。

また、「国が講ずべき個人情報の保護のための措置に関する事項」では、「(3) 分野ごとの個人情報の保護の推進に関する方針」の「① 各省庁が所管する分野において講ずべき施策」に「また、悪質な事業者の監督のため、個人情報取扱事業者に対する報告の徴収等の主務大臣の権限等について、これを適切に行使するなど、法等の厳格な適用を図るものとする。」と付け加えた[46]。法は所管が明らかでない場合は、内閣総理大臣が主務大臣を指定できることとしている[47]。しかし、詐欺を行うような「悪質な事業者」や名簿販売事業者の主務大臣は決められておらず、図 3 の中流にあたる③流通事業者や④流通・流出した情報を利用する事業者に対する対策は動かなかった。

2014 年 3 月、国会で名簿販売事業者の主務大臣について質問があっても、「特定の官庁が一律に所管しているわけではございませんので、その取り扱う個人情報の種類に応じて主務大臣が決まることになっております」と答弁されている[48]。2014 年に発生した大量漏えい事件において、窃取された情報が名簿販売事業者によって流通していたが、事件の 2 か月後に、当該漏えいした事業者から漏えいした個人情報に限定して、経済産業省が主管と指定された[49]のが最初で最後である。

消費者センターの苦情処理自体により、中流の名簿販売事業者まで遡れなくても、下流の利用事業者の中には、あっせんによって、消費者との紛争解決に対応することとなった者もいると思われる。しかし、あっせんは、結局、相手方とのコンタクトが必要であり、信用できるかどうかわからない名簿利用者と話すのは、消費者にとってはハードルが高いと思われる。

2.5 2015 年改正法による不適正な流通への対応[50]

2014 年の大量個人情報漏えい事件をきっかけに名簿販売事業者問題が社会的に注目され、また、不正に持ち出された個人情報が名簿販売事業者によって転々流通することへの国民の不安が大きくなった。

そこで、2015 年改正法では、①オプトアウト手続きによる第三者提供についての規制強化②トレーサビリティを導入した。

まず、①のオプトアウト手続きによる第三者提供の規制強化である。

形式的にオプトアウト手続きを整えていても、そもそも出自が不当な個人データの取得により本人が認識できないところで流通するため、オプトアウトの権利を行使することが不可能である。そこで、改正前から求めていた通知・公表事項に「(第三者提供の停止要請を)受け

---

[45] 前掲注 40　6 (1)②
[46] 前掲注 40　2 (3)①
[47] 2015 年改正前　法 36 条
[48] 大島他・前掲注 37、280 頁、2004 年 3 月 4 日参議院予算委員会森大臣答弁
[49] 大島他・前掲注 37、281 頁、「発覚後 2 か月以上経った同年 9 月 12 日に、当該事案に限定する形で内閣総理大臣が経済産業大臣を主務大臣として指定（旧個 36 条 1 項ただし書き）した。」
[50] 以下、改正条文の趣旨については、日置巴美＝板倉陽一郎『個人情報保護法のしくみ』74 頁（商事法務，2017）

付ける方法」を追加し、これらの事項を個人情報保護委員会に届け出させ、委員会はこれを公表することとした[51]。また、施行規則ではこれらの事項を「確実に認識できる適切かつ合理的な方法によること」とし、全く本人が認知していないところで個人データを売買する名簿事業者には遵守をほぼ不可能な条件をつけた[52]。

次に、②トレーサビリティである。

従来も、個人情報の受領者が、不正な持出による個人情報であると知りながら取得した場合であれば、不正の手段による取得として違法だった[53]が、その立証ができなかった。提供者が取得元を明かす義務や受領者が適正な取得によるものであると確認する義務もないため、拡散していく個人情報を防ぐ仕組みがなかった。更に個人情報保護委員会が立入検査などで調査するにしても、端緒から一つひとつ事業者を遡って確認しなければならないが、記録がないため調査に多大な労力がかかる。そのため、不正な個人情報の流通を阻止しつつ、個人情報の漏えい等の問題が発生した際に、委員会が取得経路について迅速に把握できるよう、トレーサビリティを確保する第三者提供の記録義務が創設された[54]。特に取得に当たっては、取得の経緯を確認する義務が付加され、適正な取得であることのより踏み込んだ確認が義務付けられた。

このように、法は不適正な流通に網をかけ、ある程度の効果はあるだろう。経緯確認義務により買取動機をけん制し、トレーサビリティで表の事業の名簿購入者から遡ることによって、見えなかった名簿事業者にも多少は網をかけることができるかもしれない。

しかし､個人情報保護委員会の Web に掲載されているオプトアウトによる第三者提供の届け出をした事業者を見ても、自分の情報が流通しているかどうかはわからないし、そこに公表されている複数の事業者に自分の情報を持っているかを確認するのも非現実的である。今回の改正で、個人情報保護委員会に、立入検査権が認められた[55]。委員会がこの権限とトレーサビリティを活かして調査してくれることを期待するが、そもそも端緒がなければ調査は始まらない。利用、流通に気がつかなければ、調査はされない。

つまり、効果的な運用のためには、以下の残課題がある；

①委員会 web 上の事業者も含め、名簿販売事業者に対する容易な開示請求

②流通・利用の検知

[51] 2015 年改正個情法 23 条 2 項 4 項
[52] 施行規則 7 条 1 項 2 号
[53] 個情法 17 条 1 項
[54] 改正個情法　25 条 26 条
[55] 改正個情法　40 条

3　セキュリティ侵害通知制度[56]

3.1 セキュリティ侵害通知制度

日本においても、個人情報の漏えい等の事案(インシデント)が発生した場合は、真面目な事業者は、関係省庁への報告、本人に対する通知、と、事実関係の公表を行っている。これは、個人情報保護法の全面施行前の 2004 年 4 月に閣議決定された「個人情報の保護に関する基本方針」とこれを受けた各省のガイドラインにおいて、二次被害の防止、類似事案の発生回避等の観点から「望ましい」とされたためである。本人に通知することにより、もし、漏えいした個人情報が悪用されコンタクトされたとしても、警戒して二次被害を防止することができる。また、通知できない場合でも公表することによって同様の効果を少しでも期待できる。公表することによって、そのようなインシデントが起こりうることを世の中に知らせ、他者で予防策を講じることが可能となる。通知がなければ、本人は漏えいが起きたこと自体を知りえない可能性がある[57]。

この考え方を世界で初めて導入したのは、2002 年成立したカリフォルニア州のセキュリティ侵害情報法[58]である。この制度は本人に漏えいの事実を通知することでセキュリティ侵害による危害を緩和する目的で作られた。その後、他の州や国に広がっている。既に、米国では 48 州が導入[59]している。また、2016 年 4 月成立した EU の一般データ保護規則においても、導入[60]されている。

3.2 米国[61]

米国では、後述するように、包括的な個人情報保護法はなく、連邦法では、必要の都度、業界ごとに法律を定めるセクトラル方式が取られている。この連邦法において侵害通知を義務付けているのは、主として健康保険ポータブライリーティ及び説明責任法[62]、アメリカ復興・再投資法[63]の一部である経済的・客観的な健康情報技術に関する法律[64]、及びグラム・リ

---

[56] security breach notification や data breach notification と呼ばれる
[57] 湯淺墾道「アメリカにおける個人情報漏洩通知法制に関する考察」情報ネットワーク・ローレビュー第 11 巻(2012 年 11 月)72-87
[58] California Security Breach Information Act (Senate Bill 1386)
[59] National Conference of State Legislation, *Security Breach Notification Laws*, Apr. 12, 2017, http://www.ncsl.org/research/telecommunications-and-information-technology/security-breach-notification-laws.aspx (2017･4･23･)
[60] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) 33 条、34 条
[61]湯淺・前掲注 57 の他、 INFORMATION SECURITY AND PRIVACY, A PRACTICAL GUIDE FOR GLOBAL EXECUTIVES, LAWYERS AND TECHNOLOGISTS, 64 (Thomas J. Shaw Esq. Ed., 2011)
[62] Health Insurance Portability and Accountability Act, P.L. 104-191, 110 Stat. 1936 (1996), codified in part at 42 U.S.C. §§ 1320d et seq.
[63] American Recovery and Reinvestment Act of 2009, P.L. 111-5, codified at 2 U.S.C. 661 et seq.
[64] The Health Information Technology for Economic and Clinical Health Act = HITECH Act, Title XIII of Division A (§§ 13001-13424) and Title IV of Division B (§§ 4001-4302) of the American Recovery and Reinvestment Act of 2009 (ARRA), P.L. 111-5.

ーチ・ブライリー法[65]の 3 法である[66]。

しかし、州法では、侵害通知は既に 48 州で導入されており、業種を問わず適用されることから、州法の影響が大きい。

米国の各州[67]においては、対象となる「個人情報」、順守義務を負う者の範囲、何が侵害に該当するか[68]、通知義務の内容、例外等は、ほぼ類似しているものの、細かなばらつきがある。

対象となる「個人情報」については、ほとんどの州において、氏名と以下の情報の組合せで漏えいした場合、としている[69]；

・ソーシャルセキュリティ番号

・運転免許証番号、及び/又は

・口座番号、クレジット番号、デビッドカード番号が暗誦番号と共に

氏名との組合せで対象となる情報としては、州によっては、電子的な ID と PW などのアクセス情報の組合せや、健康保険情報、バイオメトリックス情報、雇用主 ID、親の旧姓等を挙げるものもある。政府や自治体が公開している情報を対象外としているものもある[70]。興味深いのは、１州[71]を除き、氏名、住所、性別、生年月日の基本 4 情報だけで義務付ける州はない点である。

侵害の定義については、ほとんどの州で、暗号化又は reduct されていない電子化されたデータのオーソライズされていない取得またはアクセスにより「個人情報」のセキュリティ、機密性又は完全性が損なわれること[72]、とされている。本人に対しての危害や実際の損失がな

---

[65] Gramm Leach Bliley Act , Pub.L. 106-102, 113 Stat. 1338.

[66] 連邦法については、4.1 章に詳説する。

[67] 以下、各州の状況は、特段の注がない限り、Shaw 前掲注 61

[68] 例えば、カリフォルニア州では、以下のように定められている；
Cal. Civ. Code §§ 1798.29,
(a) Any agency that owns or licenses computerized data that includes personal information shall disclose any breach of the security of the system following discovery or notification of the breach in the security of the data to any resident of California (1) whose unencrypted personal information was･･･ acquired by an unauthorized person, or, (2) whose encrypted personal information was, ･･･ acquired by an unauthorized person (後略)

[69] 例えば、カリフォルニア州では、以下のように定められている；
Cal. Civ. Code §§ 1798.29,
(g) For purposes of this section, “personal information” means either of the following:
(1) An individual’s first name or first initial and last name in combination with any one or more of the following data elements, when either the name or the data elements are not encrypted:
(A) Social security number.
(B) Driver’s license number or California identification card number.
(C) Account number or credit or debit card number, in combination with any required security code, access code, or password that would permit access to an individual’s financial account.
(D) Medical information.
(E) Health insurance information.
(F) Information or data collected through the use or operation of an automated license plate recognition system, as defined in Section 1798.90.5.
(2) A user name or email address, in combination with a password or security question and answer that would permit access to an online account.

[70] 例えば、カリフォルニア州では、以下のように定められている；
Cal. Civ. Code §§ 1798.29,
(h) (1) For purposes of this section, “personal information” does not include publicly available information that is lawfully made available to the general public from federal, state, or local government records.

[71] ノースダコタ州

[72] Shaw 前掲 61 には“Most state statutes define a data breach as the unauthorized acquisition of and access to unencrypted or unredacted computerized data that results in the compromise of the security, confidentiality, or integrity “と、

くても通知が必要だが、経済的損失やなりすまし、詐欺、など、危害が起こりうる実質的レベルのリスクがあることなどの基準を伴っている州もある。

通知については、最も速やかに、不合理な遅滞なく通知をすることを求めている。45 日以内と明記している州もある。通知の方法は、書面、電話によるが、元の取引が電子的なものである場合等は電子的な通知も可能である。対象が多人数に上り、州法で定める基準以上のコストがかかる場合は、通知の代替手段を取ることができる。代替手段とは、自社の Web サイトと州や地方のメディアに目立つ通知を掲載することである。

いくつかの州では、一定程度以上の侵害については、州の検察や消費者保護委員会などに報告する義務もある。

例えば、NY 州の事例[73]を見てみる。

NY 州では、2005 年、General Business Law 899-aa 条に侵害通知が追加された。NY 州でビジネスをする事業者は、「private information」について、システムのセキュリティが破られたときは、その情報が暗号化されていなければ、情報を取られた(又は合理的に取られたと思われる)NY 州住民に開示しなければならない[74]。受託している事業者は、そのオーナーに通知しなければならない。

法は、まず、「個人情報」を、「名前や番号や個人のマークや他の identifier により、自然人を特定することに使われ得る自然人に関するすべての情報」とし、「private information」とは、次のデータエレメントの 1 以上のものとの組み合わさった個人情報、としている；

・ソーシャルセキュリティ番号
・運転免許証番号、又は non-driver ID カード番号、又は
・口座番号、クレジット番号、デビッドカード番号が暗誦番号と共に

そのうえで、「private information」は、連邦や地方の政府によって合法的に公にされた情報は含まない、としている[75]。

「システムのセキュリティが破られた」とは、「事業者の保有する個人情報が、権限なく取得され、又は、セキュリティ、機密性、又は完全性が有効な権限なく破られ取得されること」と定義されている。その判断要素の例として、①コンピュータやデバイスの紛失や盗難のように無権限者が物理的に保有している形跡(sign)がある、②情報がダウンロードされたかコピーされた形跡がある、③詐欺的な口座開設やなりすまし事象が報告されるなど無権限者が使っている形跡がある、ことがあげられている。

通知方法と代替手段としての公表については、前述の州法の傾向と同様である。通知のタイミングは、なるべく早く不合理な遅れなくしなければならない、が、法執行機関の合法的必要性や、被害の広がりの判断やシステムの合理的な回復に必要な手段と、整合的でなければならない、としている。4 項では、法執行機関が本人通知が刑事捜査の妨げになると判断するときは、通知は遅らせてもよい、としている。

セキュリティと機密性、完全性が並列に書かれている。

[73] Office of NY Attorney General, INFORMATION EXPOSED Historical Examination of Data Breaches in New York State, 2014, https://ag.ny.gov/pdfs/data_breach_report071414.pdf (2017･6)

[74] 899-aa 条 2 項

[75] 899-aa 条 1 項〔a〕〔b〕

更に、州住民に開示しなければならない時は、州検察、Department of State (州内務庁)、州警察に、通知しなければならず、5000 人以上の NY 州住民が影響を受けた時は、州消費者保護委員会にも報告しなければならない[76]。報告フォーマットは、図 8 のとおりである。このほか、State Technology Law208 条に基づき、別の州政府機関にも報告しなければならない。

このように、本人への開示義務がメインで、最後に州検察などの機関への開示義務が書かれている。本人への通知は本人の自衛を促すためだと考えるが、州の機関への開示義務の目的は書かれていない。また、前述のように、州政府への報告を義務づけている州は少数派のようである[77]。しかし、検察等の捜査機関であるということは、届け出をする事業者を取締る目的ではなく、取得された情報の詐欺などでの利用や不正アクセスや窃取などの犯罪行為の捜査が目的と考えられる。報告先の機関については、899-aa 条 8 項〔b〕は consumer reporting agencies（消費者保護委員会）への報告義務を定めるが、州の報告資料の説明[78]は、credit reporting agencies(Eqifax, Experian, and TransUnion)に報告すべし、と書かれている。また、Shaw は、州検察、州消費者保護委員会、州サイバーセキュリティ室、Critical Infrastructure and Coordination にも通知が必要、と説明している[79]。これらから判断すると、やはり、目的は取得された情報の詐欺などでの利用や不正アクセスや窃取などの犯罪行為の捜査と考えられる。州法で一般的な安全管理義務がないため、漏えいを起こしてしまった事業者を裁く方法もないこともあろうが、合理的な制度と考える。

[76] 899-aa 条 8 項

[77] Shaw・前掲注 61　67 頁　は“Some states, such as Indiana, Maryland, Massachusetts, New Hampshire, and New York include provisions for notice to the state attorney general for some breaches, in addition to affected individuals.”と記述する。

[78] 前掲注 73　18 頁

[79] Shaw・前掲注 61　67 頁

APPENDIX D: NEW YORK STATE SECURITY BREACH REPORTING FORM

NEW YORK STATE SECURITY BREACH REPORTING FORM

Pursuant to the Information Security Breach and Notification Act
(General Business Law §899-aa)

Name and address of Entity that owns or licenses the computerized data that was subject to the breach:
Street Address: _____
City: _____ State: _____ Zip Code: _____

Submitted by: _____ Title: _____ Dated: _____
Firm Name (if other than entity): _____
Telephone: _____ Email: _____
Relationship to Entity whose information was compromised: _____

Type of Organization (please select one): [ ] Governmental Entity in New York State; [ ] Other Governmental Entity; [ ] Educational; [ ] Health Care; [ ] Financial Services; [ ] Other Commercial; or [ ] Not-for-profit.

Number of Persons Affected:
Total (Including NYS residents):_____ NYS Residents:_____
If the number of NYS residents exceeds 5,000, have the consumer reporting agencies been notified? [ ] Yes [ ] No

Dates: Breach Occurred:_____ Breach Discovered:_____ Consumer Notification:_____

Description of Breach (please select all that apply):
[ ] Loss or theft of device or media (e.g., computer, laptop, external hard drive, thumb drive, CD, tape);
[ ] Internal system breach; [ ] Insider wrongdoing; [ ] External system breach (e.g., hacking);
[ ] Inadvertent disclosure ; [ ] Other specify): _____

Information Acquired: Name or other personal identifier in combination with (please select all that apply):
[ ] Social Security Number
[ ] Driver's license number or non-driver identification card number
[ ] Financial account number or credit or debit card number, in combination with the security code, access code, password, or PIN for the account

Manner of Notification to Affected Persons - ATTACH A COPY OF THE TEMPLATE OF THE NOTICE TO AFFECTED NYS RESIDENTS:
[ ] Written [ ] Electronic [ ] Telephone [ ] Substitute notice
List dates of any previous (within 12 months) breach notifications: _____

Identity Theft Protection Service Offered: [ ] Yes [ ] No
Duration: _____ Provider: _____
Brief Description of Service: _____

図 8　ＮＹ州　侵害通知フォーム

3.3 日本

個人情報保護法が成立したのは 2003 年 5 月だが、2004 年 4 月 2 日、個人情報保護法の全面施行時に先立ち個人情報保護政策の総合的な基本方針として、「個人情報の保護に関する基本方針[80]」が閣議決定された。その中で、個人情報の漏えい等の事案が発生した場合は、「二次被害の防止、類似事案の発生回避等の観点から、可能な限り事実関係を公表することが重

[80] http://www.soumu.go.jp/main_sosiki/joho_tsusin/policyreports/chousa/hoso_it_eisei/pdf/040510_2_s1-5-5_5.pdf (2017･4･25･)

要」とされた。これは、世界で初めて breach notification を定めたカリフォルニア州のセキュリティ侵害情報法が日本の個人情報保護法成立後の直後に成立し、その制度を導入しようとしたものである。

1990 年以降進んだ規制緩和下で、事前規制から事後規制、官の行政指導に頼った法規範から自己責任規範への大きな流れの中、とりわけ、高度情報化社会化に伴う法的秩序は、技術の発展やこれに伴う新たな事業の発展を阻害しないために、この考え方が強かった。この事後規制、自己責任の流れからは当然かもしれないが、2000 年に発生した雪印集団食中毒事件[81]など、不祥事自体よりも不祥事を隠蔽する企業体質が社会的に問題となった。このような流れの中、2004 年に発覚した Yahoo！BB の顧客情報漏えい事件においては強気で知られる孫社長が記者会見を行うなど、早期に公開することが社会的批判を鎮静させる事象も見られた。また、電子掲示板の普及などにより、様々な大小の不祥事が内部告発や消費者などの書込みにより明るみに出、また、マスコミがこれを取り上げることにより、自ら開示しなかったことが隠ぺいと捉えられ、レピュテーションリスクが大きくなる、という現象が出てきた。

このような時代背景の中で、この基本方針が定められた。これを受けて、例えば経済産業省のガイドラインでも、「事故又は違反について本人へ謝罪し、二次被害を防止するために、可能な限り本人へ連絡することが望ましい[82]」、とされ、本人通知、官庁報告、公表の 3 点セットが「望ましい手法の例示」としてではあるが、定められた。いずれもガイドライン的な性格[83]であり、拘束力はないが、米国の州のような合理的な個人情報の定義もない中、真面目な事業者は、レピュテーションリスクを恐れ、氏名・住所・電話番号のリストの紛失など、些細なインシデントであっても役所報告、本人通知、Web サイトなどでの公表を行うようになった。

当初は歓迎していた関係官庁も、些細なものまで都度報告する負担を合理化すべく、例えば 2009 年の経済産業省ガイドラインでは、ファクシミリやメールの誤送信（宛名及び送信者名以外に個人情報が含まれていない場合）は月 1 回まとめて報告でも可、とした[84]。また、公表については、二次被害の防止、類似事案の発生回避等の観点から、個人データの漏えい等の事案が発生した場合は、可能な限り事実関係、再発防止策等を公表することが重要とされたが、影響を受ける可能性のある本人すべてに連絡がついた場合、・紛失等した個人データを、第三者に見られることなく、速やかに回収した場合、高度な暗号化等の秘匿化が施されている場合、漏えい等をした事業者以外では、特定の個人を識別することができない場合など、二次被害の防止の観点から公表の必要性がない場合には、省略可能とした[85]。

また、プライバシーマーク制度も、侵害通知の普及に貢献した。2006 年、JIS Q 15001 が

---

[81] http://www.meg-snow.com/corporate/history/popup/oosaka.html (最終閲覧 2017 年 4 月 23 日)

[82] 経済産業省、「個人情報の保護に関する法律についての経済産業分野を対象とするガイドライン」(平成 26 年 12 月 12 日厚生労働省・経済産業省告示第 4 号)28 頁

[83] 本来、基本方針は法的拘束力のないガイドライン的性格。岡村久道『個人情報保護法〔新訂版〕』122 頁（商事法務、2009 年）
経産省ガイドラインも「『望ましい』と記載されている規定については、それに従わなかった場合でも、法の規定違反と判断されることはない」とする。前掲注 82 1 頁

[84] 個人情報の保護に関する法律についての経済産業分野を対象とするガイドライン
(平成 21 年 10 月 9 日厚生労働省・経済産業省告示第 2 号）29 頁

[85] 経産省・前掲注 82

個人情報保護法に合わせて改定された際、「緊急事態への準備」の項目が入った[86]。そこでも、個人情報の漏えい、滅失又は毀損が発生した場合に備え、対応手順を確立することが求められ、具体的に、本人への通知又は容易に知りうる状態に置くこと、二次被害の防止、類似事件の回避などの観点から可能な限り事実関係、発生原因、対応策を遅滞なく公表すること、関係機関に直ちに報告することが、挙げられている。解説書[87]によれば、「関係機関」とは、報告すべき利害関係を有している機関、という意味である。これは、事業者の判断だが、プライバシーマーク付与を受けている事業者は、審査を受けた機関や主務大臣又は認定個人情報保護団体に所属している場合はその団体を含む、とされている。これらすべての措置の実施が要求されるわけではなく、法的に義務付けられていない場合は、経済的な不利益及び社会的な信用の失墜、本人への影響などのおそれを考慮し、どういう場合にどのような措置を講じるか定めておく、とされている[88]。

2017 年 5 月 30 日より施行された改正個人情報保護法のガイドラインでも、漏えい等事案が発覚した場合は影響を受ける可能性のある本人への連絡、事実関係等の公表、が望ましいとし、個人情報委員会（認定個人情報保護団体の対象事業者については、当該認定個人情報保護団体）に速やかに報告するよう努める、とされる[89]。但し、高度な暗号化等の秘匿化、閲覧されないうちに回収、事業者以外では特定の個人を識別できない場合（但し、それのみで本人に被害が生じる恐れがある場合を除く）等、実質的に個人データが漏えいしていないと判断される場合や、FAX、メールの誤送信、荷物の誤配等の軽微なものは、報告不要としている[90]。

日本では、マイナンバーについては、法律で侵害通知が義務付けられた。マイナンバー法[91]28 条の 4 において、「個人番号利用事務等実施者は、個人情報保護委員会規則で定めるところにより、特定個人情報ファイルに記録された特定個人情報の漏えいその他の特定個人情報の安全の確保に係る重大な事態が生じたときは、委員会に報告するものとする。」とされた。重大な事態とは：

① 情報提供ネットワークシステム等又は個人番号利用事務・個人番号関係事務を処理するために使用する情報システムで管理される特定個人情報が漏えい等した事態
② 漏えい等した特定個人情報に係る本人の数が 100 人を超える事態
③ 特定個人情報を電磁的方法により不特定多数の者が閲覧することができる状態となり、かつ閲覧された事態
④職員等が不正の目的をもって、特定個人情報を利用し、又は提供した事態

とされている[92]。

また、本人通知と公表、及び重大な事態と確定する前の個人情報保護委員会への報告につい

---

86 JIS Q 15001 2006　3.3.7
87 財団法人日本情報処理開発協会『JIS Q 15001:2006 をベースにした個人情報保護マネジメントシステム実践のためのガイドライン［第 2 版］』74 頁
88 日本情報処理開発協会　前掲注 87　70 頁
89 個人情報保護委員会「個人データの漏えい等の事案が発生した場合等の対応について」（平成 29 年個人情報保護委員会告示第 1 号）
90 前掲注 89　3.(2)。この位置であれば、本人通知と公表には適用されない。これらは「望ましい」であり、委員会報告は「努める」だからか。
91行政手続における特定の個人を識別するための番号の利用等に関する法律
92 特定個人情報保護委員会規則第五号　2 条

ては、行政機関等・地方公共団体等については義務[93]、民間については推奨[94]となっている。

3.4 欧州

欧州において、侵害通知が初めて規定されたのは、2002 年の EU 電子通信プライバシー指令の 2009 年改正である[95]。改正後の第２条(h)号は、「個人データ侵害」を、「共同体内において、公に利用な電子通信サービスの提供との関係で、送信され、保存され、又は取扱われる個人データへの偶発的又は違法な破壊、紛失、無権限開示又はアクセスをもたらすセキュリティ侵害をいう」とし、改正後の第 4 条第 3 項[96]は、個人データ侵害の場合、公衆電子通信サービスプロバイダは、遅滞なく所管の国家機関に通知し、データ侵害が加入者又は個人データもしくはプライバシーに有害な影響を与える見込みがある場合、加入者又は個人にも侵害を通知することを義務付けている。前文では、これは、早く通知することによって、個人が必要な注意を取ることができるからである、と説明し、「有害な影響」は、なりすまし、物理的侵害、名誉に対する重大な侮辱又は侵害、などが例示されている[97]。第４条第３項は、通知の内容も定めている[98]。個人に対しては、侵害の性質、追加情報が必要な時のコンタクトポイント、悪影響を緩和するための方法を推奨する必要がある。また、監督官庁に対しては、これに加えて、侵害(事故)の結果と、事故に対処するために提案し又は実施した措置も報告しなければならない。なお、技術的対策によって、漏えいした情報が読めない場合は、個人への通知は不要としている。

興味深いのは、すべての侵害を監督官庁に報告することを義務付けているが、個人への通知は、有害な影響を与える場合、に限定している点である。前文の説明[99]によると、セキュリティは重要であり、政府は個人情報やプライバシーの高いレベルの保護の確保等により市民の利益を促進すべきでる。このために、個人情報のセキュリティインシデントの包括的な信頼できるデータを持つことを含めた必要な手段を持たねばならないし、取られた対策をモニターし、他の公衆電子通信サービスプロバイダにベストプラクティスを普及しなければならない。従って、公衆電子通信サービスプロバイダは、監督官庁が更なる分析や評価ができるよう、個人データ侵害の記録を維持しなければならない、としている。ここで注意しなければならないのは、この指令はあくまでも国別通信サービスの開放をにらんだ標準化の一環として、公衆通信事業者による加入者のプライバシーや通信の秘密の保護の標準化を定めたものを改正したものであり、監督官庁は DPA ではなく、通信を担当する行政機関である。監督

---

[93]平成 26 年特定個人情報保護委員会告示第６号
[94]平成 27 年特定個人情報保護委員会告示第２号
[95] 以下、石井夏生利『新版　個人情報保護法の現在と未来』（勁草書房、2017）138 頁による
[96] Directive 2009/136/EC of the European Parliament and of the Council of 25 Nov. 2009、第２条４項(c)
[97] *id*, 前文(61)
なお、2014 年、第 29 条作業部会は、いかなる場合に通知が必要かを具体的にあげた意見を出しているが、この説明よりかなり幅広い。WP213,　Opinion 03/2014 on "Personal Data Breach Notification
[98] 2013 年、委員会は通知について、regulation を出している。そこでは公衆電子通信サービスプロバイダから監督官庁への報告を 24 時間以内とし、対官庁、対個人とも、報告内容の詳細を定めている。COMMISSION REGULATION (EU) No 611/2013 of 24 June 2013 on the measures applicable to the notification of personal data breaches under Directive 2002/58/EC of the European Parliament and of the Council on privacy and electronic communications
[99] Directive 2009/136.　前文　(57)、(58)

官庁として通信事業者のセキュリティを監督し、ベストプラクティスを共有することは、可能であり、自然な行動であろう[100]。

一般データ保護規則では、業種を限定することなく、第 33 条で、個人情報保護の監督官庁への報告を義務付け、第 34 条で本人への通知を義務付けている。

監督官庁へは、セキュリティ侵害発見後 72 時間以内に通知が必要である。本人の権利と自由にリスクを与えない場合は除く、とされているが、それがどのレベルかは明記していない[101]。興味深いことに、通知の項目に、セキュリティ侵害の考えられる結果、や、悪い効果を緩和する方法等、侵害に対して取ろうとしている対策も、含まれている。

本人への通知は、本人の権利と自由に高いリスクが発生しうる場合に義務付けられており、政府への報告より限られている。また、技術的に解読できない措置が施されている場合、コントローラが対策を打って権利や自由へのリスクが実質的でなくなった場合は、通知不要としている。また、個別の通知が不相応な努力を要する場合は、本人が同様に知ることができるなら公表で代替可能である。

最近は、個人データの侵害のみならず、セキュリティ侵害全般についての通知義務を定める法律が出現している。例えば、オランダでは、2016 年 11 月に新たにデータ処理及びサイバーセキュリティ通知義務法義務法(Data processing and Cybersecurity Notification Act)において、政府が指定する必須事業者（製品またはサービスの事業者であって、その可用性及び信頼性がオランダ社会にとって必須の重要性を有しているもの）に対しては、マルウェア感染その他のインシデントの発生時に治安・法務省の下にある国家サイバーセキュリティセンター(NCSC)に届け出ると共に、必要なデータを提供することを義務づけている。その届出に基づき、NCSC がインシデント対応の支援を行う仕組みが整っている。

3.5 小括

この 3 地域のセキュリティ侵害通知に関する法を簡単に比較すると、表 5 のとおり、①法的強制力、②対象、③公表の位置づけ、④官庁報告の位置づけに違いがある。

日本は拘束力のないガイドライン的位置づけだが、米国、EU では法的義務である。2009 年の経済産業省ガイドラインや 2017 年の個人情報保護委員会のガイドラインでの緩和的措置を見てもわかるように、真面目な事業者は FAX の誤送信でも報告してきた。一方で、法的義務ではないので、全くこれらを行っていない事業者も多くあると考える。中には SNS など

---

[100] 前文(59)では、個人データのセキュリティや侵害時に個人が被る損害は公衆電子通信サービスプロバイダからの漏えいに限らないので、侵害通知義務を全業種に拡大すべきであり、委員会はこれを奨励するような妥当な措置を取るべきである、としている。

[101] 前文（85)から(88)が breach notification に関する説明だが、そこにも手掛かりはない。
一方、前掲注 97　WP213 では、公衆電子通信サービスプロバイダ以外の事例もあげており、冒頭に、「Directive 2002/58/EC は公衆電子通信サービスプロバイダにしか適用されないが、データ保護規則案の脈絡から他の業界の事例を挙げてすべてのデータ管理者にとって良いプラクティスを示している」と言及している。これが今後の参考とされるだろう、との指摘もある。加藤隆之「情報流通時代の個人データに関する『新たな権利』」ビジネス法務 2017.8、27 頁、30 頁(2017)

で騒ぎになって公表した事業者もあろうが、ある程度知名度がある事業者でなければそのような事態も起こらない。

次に通知の対象である。日本の場合は、すべての個人情報であり、したがって、FAX 誤送信も対象になってしまう。米国州法は、なりすましや経済的損害につながりうる情報とともに漏えいした場合に限定しているところがほとんどである。欧州は監督官庁への報告はほとんどの場合必要だろうが、本人への通知はリスクが高い場合に限定している。尤も、何をもってリスクが高いと判断するのかは、GDPR 自体には手掛かりが明記されていない。2014 年に第 29 条作業部会が出した意見[102]では、クレジットカード番号や健康情報などが数百件以上流出した事例は挙げられているが、通知が不要な例としては暗号化しか挙げられておらず、判断に迷うような事例の指針としては、物足りないが、少なくとも日本のように FAX の誤送信のようなものは考えていなさそうである。

公表の位置づけも違う。米国と欧州は数が多いなど、本人通知が不相応に負担となる場合にその代替手段として公表することができる、という位置づけだが、日本は、本人通知と並列である。

表 5　侵害通知制度の国際比較

		米国	EU	日本
法的義務？		義務	義務	推奨(義務ではない)
対象となる個人情報		なりすましリスクのある重要な情報との組み合わせ 暗号化除く	限定無し	限定無し
内容	本人通知	義務	権利及び自由に対して高リスクを引き起こし得る場合 (暗号化等除く)	（漏えい等事案の内容等に応じて）
	公表	通知が負担の場合の代替手段	通知が負担の場合の代替手段	並列 （漏えい等事案の内容等に応じて）
	官庁報告	一部の州 (なりすまし捜査材料か)	（自然人の権利又は自由に対するリスクが生じ得ない場合を除く）	以下を除く ①実質的に外部に漏えいなし ②軽微な誤送信

また、文化的なものかもしれないが、通知の目的に謝罪が入っていたのも日本だけである。

官庁報告の位置づけも興味深い。米国は本人通知でまず本人の利益を図り、官庁報告まで求める州が多いわけではない。報告先は州検察や消費者保護委員会で、取られた情報の不正

[102] 前掲注 97　WP213

利用や不正アクセスの捜査が目的と思われる。日本では、本人通知、官庁報告、公表の順に記述されている[103]。日本の場合、事業者に安全管理義務があり、主務大臣制を取っていたので、官庁報告は法の広い意味での執行のため、と考えられる。

欧州は、まず官庁報告があり、その後で本人通知を定めている。電子通信プライバシー指令の時代は、前述のとおり、通信事業者を監督する立場から、すべての把握とフォローのため、報告を義務付け、取られた対策をモニターし、他の公衆電子通信サービスプロバイダにベストプラクティスを普及することを目的としていた。しかし、GDPR は個人情報保護の監督機関（supervisory authority）への報告を義務付けている。監督機関がすべての業種について、通信事業者の監督と同様の監督を行うのか疑問に思うが、個人情報保護指令下で定めていた個人情報取扱すべてについての監督機関に対する通知義務が負担だけで効果を上げなかったことから、対象を絞って侵害通知制度を導入したものである、との説明[104]は、EU の官僚主義的拘りとして理解できる。報告を受けてどうするか、が、重要であろう。前述の、オランダにおける必須事業者に対しサイバーセキュリティインシデントの報告義務を定めた法律も、同様に、国家の監督により社会基盤を守ろうとするものと考えられる。日本やアメリカは、重要インフラ事業者の官民連携の一環として、サイバーインシデントやその手口や対策の共有を国家の政策として行っている[105]。監督官庁が重要インフラ事業者を把握し管理している場合は法的義務は不要かもしれないが、海外事業者や小さな事業者やアウトサイダーなど、把握できず、または、協力しない者まで対象とすべき時は、表 1 に示すように法律上の義務にすることが必要になるのかもしれない。

最近発表された研究[106]では、州の侵害通知義務への enforcement がよく行われている州、報告する事業者にインセンティブがある州、社内ポリシーで顧客に通知することを決めている事業者を報告義務から免除している州で、なりすまし事件が少ない、ということが報告されている。このように、重要な情報の漏えいについての本人への通知は意味がある。

今後、日本でも義務化が検討されると思われるが、現在のままでそのまま義務化となると、合理性も問われることにならないだろうか。本人への通知は、二次被害の防止という観点からは合理的だが、謝罪については、現実には伴うとは思われるが、法的義務に馴染むか検討が必要である。また、すべての個人情報を対象として法的義務とするとのか、全事業者にどんな情報セキュリティインシデントでも法的義務を負わせるのか、を整理する必要がある。前述した JIS Q 15001 の解説書の説明程度のリスク判断の余地は最低限必要であろう。個人

---

103 経産省、前掲注 82　29 頁

104 石井　前掲注 95、140 頁。前文(89)を引用。(89)はプライバシーインパクトアセスメントの説明でもある。

105 日本では、2005 年「重要インフラの情報セキュリティ対策に係る行動計画」の中に「情報共有体制の強化」もあったが、2012 年 4 月、東日本大震災発生時における複数の IT システムの同時的障害発生や IT システムに対するサイバー攻撃などの環境変化を踏まえた「重要インフラの情報セキュリティ対策に係る第２次行動計画 改定版」では、BCP（事業継続計画）などの充実、環境変化を踏まえた安全基準の改善、情報共有体制の強化などが内容に盛り込まれ、事故情報の共有が進んだ。2015 年 1 月にサイバーセキュリティ基本法の施行に伴い体制強化され、「重要インフラの情報セキュリティ対策に係る第３次行動計画」でも「重要インフラ事業者の自主的な対策として期待する事項」の情報共有体制の強化では、②ＩＴ障害発生時等に必要に応じて情報連絡、③攻撃手法及び復旧手法に関する情報等の収集　が挙げられている。

106 FEDERAL RESERVE BANK OF KANSAS CITY, Data Breach Notification Laws, 2016, https://www.kansascityfed.org/~/media/files/publicat/econrev/econrevarchive/2016/1q16sullivanmaniff.pdf　(2017･6)

情報保護委員会への報告についても、その目的を明確にすべきである。類似事案の発生回避目的であれば、本来、一般に知られないような手口や質、量のものや、サイバーインシデントのような手口が次々と変わるものだけでよいはずで、FAX 誤送信、PC の紛失、盗難など、既に社会的によく知られたものは不要なはずである。その判断を任せられないから、立法論としては原則報告とするのだろうが、届け出不要の範囲をもっと広げるべきである。公表についても、その目的を再検討すべきである。二次被害の防止は通知でよく、類似事案の発生回避という意味では、知らせる価値のある事案について、報告された政府の発表を介せばよい。認定個人情報保護団体がカバーしていない中小企業や個人事業主がセキュリティ侵害発生時に届出をしやすい窓口整備も必要だろう。

ただ、確かなことは、事業者が漏えいに気づかなければ通知もできない、ということである。

4　米国における個人情報保護規範の「執行」状況

4.1　米国の個人情報保護規範概要

4.1.1 プライバシー権の確立

「プライバシー権」は 19 世紀後半、米国で発祥した[107]。　1880 年、クーリー判事による「不法行為法論」において、「一人で居させてもらう権利」という概念が登場したが、法的権利という意味合いにいて最初に現れたのは、サミュエル・D・ウォーレンとルイス・D・ブランダイスが 1890 年に発表した論文「プライバシーの権利」[108]であった。英国を発祥とする近代的な新聞は、民主主義の発展と拡大に伴い、米国でも市民階層を読者として広がったが、19 世紀になると、読者の興味を引くニュースや読み物に内容をシフトすることで、急速に発行部数を伸ばし、大衆報道新聞を発行する企業活動の側面も出てきた[109]。これにより、個人的な事柄まで子細に書き立てられ、また、記者によるスナップ写真の撮影も可能となった時代背景から、困惑するケースが増えてきた。そこで、ジャーナリズムによる私生活や家庭生活の神聖な領域への介入に対し個人を保護する権利を提唱し、「ひとりで居させてもらう権利（the right to be let alone）として、プライバシーの権利を不法行為上の観念として登場させた。

プライバシーの権利が争われた初めてのケースは、1902 年、ニューヨーク州最高裁判所のロバーソン事件[110]だった。肖像を無断で自社の製品の宣伝用に大量配布され、それに気づいた周囲の者から冷やかしや嘲りを受けて心身に多大な苦痛を受け、病気になって通院せざるを得なくなったとして宣伝用の印刷物の頒布差止と損害賠償を請求したこのケースでは、プライバシーの権利は存在しない、として、4 対 3 で原告の請求を棄却した。理由としては、これを認めた時に今後膨大な訴訟が予想されること、出版の自由の過度の制限への懸念があげられている。

その後、直ちに激しい世論の反応があり、翌年、ニューヨーク州議会は、初めて制定法によるプライバシーの権利を認めた。

その後、1905 年、ジョージア州最高裁判所が、ペーブジック事件[111]において、初めてプライバシーの権利を判例上で承認した。これも自分の写真を勝手に新聞広告で使われた事件で、判決は、ウォーレンとブランダイスの考えの多くを取り入れ、プライバシーの権利を自然権に基づくものとして、州憲法の幸福追求権を根拠に、不法行為上の権利として承認した。

1931 年には、カリフォルニア州最高裁判所においてメルビン事件の判決があった。被告は、原告の非公知の過去（かつて売春婦であり、世間を騒がせた殺人事件の被告人として裁判を受けたが無罪となったこと）を題材とした実名入りの映画を上映し、更生し結婚し平穏な生活を送っていた原告の過去が暴露され、新生活が破滅に至ったケースである。裁判所は、「プライバシーはひとりで居させてもらう権利」として、「更生した後に・・公表したこと」は、

---

107 米国法の発展については、岡村久道＝新保史生『電子ネットワークと個人情報保護－オンラインプライバシー法入門―』35 頁（経済産業調査会、2002）

108 S.D.Warren & L.D. Brandeis, *The Right to Privacy*, 4 HARV. L.REV.195(1890)

109 松井茂記『マスメディア法入門〔第２版〕』(日本評論社、1998)1 頁

110 Roberson v. Rochester Folding Box Co.. 171 N.Y. 583, 64 N.E. 442 (1902)

111 Pavesich v. New England Life Insurance Co. 122 Ga. 190 50S, E. 68 (1905)

州憲法上の幸福追求権の侵害、として、プライバシー権を認めた。

この後、同様の判例が増加し、多くの州の裁判所でプライバシー権を認めることが一般的になったが、内容も学説も多様であった。そこで、ウィリアム・L・プロッサー教授が 1960 年発表した論文「プライバシー」[112]において、判例を次の類型に整理した。

①INTRUSION (私生活への侵入：原告がひとりで他人から隔絶されて送っている私的な生活状態への侵入)

②PUBLIC DISCLOSURE OF PRIVATE FACTS（私事の公開：原告が知られたくない私的な事実の公開）

③FALSE LIGHT IN THE PUBILC EYE（誤認を生じる表現 : 原告について一般の人に誤った印象を与えるような事実の公表）

④APPROPRIATION （私事の営利的使用：原告の氏名又は肖像を、被告の利益のために盗用すること）

そして、各州の判例法から法理を整理した第二次リステイトメントでも同様の 4 類型が示され、分類についての議論はあるものの、判例においても実務においても確立している。

4.1.2 個人情報保護の要請への立法による対応

1970 年代、電算化が進み「ビッグブラザー」による監視の懸念から個人情報保護が問題になった時期、建国の経緯から政府の手を縛ることは重視する米国では、1974 年、連邦政府の保有する個人情報を保護するプライバシー法[113]が成立した。

この法律は、政府による個人に関する情報の収集、利用、管理、セキュリティを規制している。政府は政策目的を達成するために必要で、関係があり、正確でタイムリーな情報のみを集めることができる。集めた情報は、記録システムに保存しなければならならず、そこに適切な個人情報保護措置を講じなければならない。情報主体に対し、記録システムに登録されている個人情報へのアクセス権を認め、情報の変更を求めることができる。各政府機関は、記録システムについて、名称、個人情報の種類、利用目的や日常的業務での使用それぞれの内容、情報源と情報の種類、と共に、システムに自らの情報が含まれていることを知るための手続きやアクセス方法、内容への異議申立方法などを公にすることが義務付けられている。

連邦政府のセキュリティに関しては、その後、Government Information Security Reform Act (GISRA)が定められ、更に 2002 年、The Federal Information Security Management Ac[114]t (FISMA)が成立している。そこでは、単なるリスクベースでのセキュリティから、機密性、可用性、完全性概念に基づいて規定されるようになった。各機関は、国防や諜報に関する者を除き、Office of Management and Budget (OMB)に対し、リスクアセスメント、セキュリティポリシー、計画、訓練、テストと評価、改善、インシデント報告、事業継続について、報告義務がある[115]。

この他、必要に応じ、大統領令で具体的な要件、施策を出している[116]。

---

112 William L. Prosser, *Privacy,* 48 CALIF. L. REV. 383 (1960)

113 Privacy Act of 1974, Pub. L. No.93-579

114 Federal Information Management Act of 2002, Pub L.No. 107-343, Title III, 116 Stat. 2899 (2002) (amending 44 U.S.C. section § § 3541-49)

115 44 U.S.C. § 3544(b)(5)

116 例えば、2017 年 5 月 11 日、Executive Order titled “Strengthening the Cybersecurity of Federal Networks and Critical

しかし、民間の事業の自由を重視する米国では、欧州とは違い、連邦レベルで包括的な個人情報保護法は制定されていない。民間については、自由な情報流通の確保を前提としたうえで、必要性が出た都度、個別分野ごとにプライバシー保護を目的とした法律を制定するセクトラルアプローチを取っており、連邦法だけで約 30 の法律が制定され、連邦機関や民間企業への義務を課している[117]。包括的な個人情報保護法に至らない背景には通信販売業者やデータブローカーの政治力があると言われている[118]が、訴訟社会の米国で概念から発した制定法を作ること自体がリスクと感じられていた面もあろう。

セクトラル方式で制定されている法律のいくつかを紹介する。

まず、金融分野について。1978 年、金融プライバシー法が制定されたが、これは金融機関の持つ個人情報を連邦政府が入手できないようにするためのものであった。1999 年、金融サービス近代化法（Gramm-Leach-Bliley Act (GLBA[119])）が、1932 年制定の Glass-Steagall Act を置換え、銀行と証券の垣根を取り払った際、金融機関の個人情報の取扱についても規定を置いた。

金融機関にプライバシー保護方針を明示することを義務付け、消費者が自らの個人情報の利用に関する選択を行う際に指針となる情報の提供を義務付けている。2009 年金融機関を規制する 7 つの政府機関と FTC が、法の通知義務を満たす model privacy notice form を出している[120]。

また、この法は、情報セキュリティについても、金融分野で守れる範囲の注意義務を定め、金融分野の監督機関に対し、機密性と完全性を守るために適切な基準を定めることを義務付けている[121]。これに基づき、2001 年、銀行を規制する機関が合同で最初の統一ガイドラインを出している[122]が、これは法律上の義務であり、違反に対してはこれらの機関が強制力を持つものである。また、このガイドラインの中に、顧客情報への不正アクセスに対する対処と顧客への通知プログラム（Interagency Guidance on Response Programs for Unauthorized Access to Customer Information and Customer Notice）が含まれており、侵害通知が義務付けられている[123]。

健康分野においては、1996 年の「健康保険の相互運用性及び説明責任に関する法律[124]」において、医療機関や健康保険を扱う事業者に対し、患者の医療記録・保険記録に関連するデータの管理、保護に注意を払うよう求め、Department of Health and Human Service (HHS)に電

Infrastructure” が出され、各機関に NIST の Framework for Improving Critical Infrastructure Cybersecurity への計画の義務付けなど 政府 IT のサイバーセキュリティ対策強化、重要インフラのサイバーセキュリティ強化、国際連携などを定めている。

117 湯淺・前掲注 57　75 頁

118 岡村＝新保・前掲注 107、121 頁では、1990 年代、インターネットの発達により、容易に大量の個人情報を収集できることから、一定の規制を導入すべき、との議論があった際、この規制に反対する活動団体のひとつである情報の公正利用連合（Fair Information Practices Coalition）は、投資企業協会、信用情報機関連合、証券取引業協会、ダイレクトマーケティング協会、アメリカ保険業協会の支援を受けていた、と紹介している。
湯淺前掲注 57　74 頁でも、「各業界がそれぞれの事業形態が特殊であり、包括的な規制には適さないと長年主張してきたため」とし、The Privacy Protection Study Commission, *Personal Privacy in an Information Society The Report of The Privacy Protection Study Commission, July, 1977* を引用している。

119 Financial Services Modernization Act of 1999, Pub L.. No.106-102, 113 Stat. 1338 (1999)

120 74 Fed. Reg. 62890 (Dec. 1, 2009)

121 Sec.501(b)

122 Interagency Guideline Establishing Standards for Safeguarding Customer Information, 66 Fed. Reg. 8616 (Feb. 1, 2001)

123 湯淺　前掲注 57　77 頁

124 Health Insurance Portability and Accountability Act of 1996, P.L. No.104-191 (42 U.S.C. §1320d-2)

子的な医療情報の取扱に関する国家基準を制定することを義務付けている[125]。これに基づき、プライバシールールとセキュリティルールが行政規制として定められている。プライバシールール[126]は、保護すべき健康情報（protected health information (PHI) ）について、電磁的情報だけでなく、口頭や紙の情報にも適用される。プライバシールールでは、一定の例外を除いて患者の承諾なく患者の健康情報を利用したり第三者提供することを禁じ、利用できる場合や開示できる場合を限定し、最小限の情報提供の方法や Business Associate への開示についても定めている。監督機関に、Privacy Official を届出て、プライバシールール順守のためのポリシーと手続きを定めることを求めている。セキュリティルール[127]では電磁的健康情報(e-PHI)の保存、通信、受信における機密性、完全性、可用性の保持を義務付け、リスク分析に基づき、技術的、物理的、人的管理を行うことを義務付けている。

2009 年、アメリカ復興・再投資法[128]の一部として、経済的・クリニカル健康情報の技術に関する法律[129]が制定され、侵害通知義務が具体的に定められた。

この他、1984 年のケーブル通信政策法[130]では、本人の同意なしに加入者の視聴傾向を第三者に開示することを禁止し、1988 年のビデオプライバシー法[131]では、レンタルビデオの貸し出し情報の開示が禁止されているが、いずれも、問題が発生して対応したものである。

州法においては、プライバシー権について、州の憲法に定める州は多いが、個人情報保護に関する法律は、前述の侵害通知を除き、連邦同様に個別領域毎のセクトラル方式である[132]。多くの州が定めているのはソーシャルセキュリティ番号の取扱に関する法である。その使用は最小限にすることや合法的目的なく開示しないこと、セキュリティの確保等が定められている。また、個人情報一般について、廃棄時に漏えいしないような手立てをとること、程度の義務を定めた Data Disposal Laws を持つ州も複数ある[133]。

4.1.3 FTC による規制[134]と「プライバシー・コモンロー[135]」

米国の個人情報保護規範において、最も興味深くダイナミックなのは、FTC による規制である。

FTC は、1914 年の FTC 法によって設立された独立行政委員会で、その法の授権範囲で Rulemaking 権も、取締り強制する権能もある。元々は反競争的行為への対応が目的だったが、1938 年に「不公正または欺瞞的な行為または慣行」への対応が目的に追加された。

現在、委員会のもとに、消費者保護局（Bureau of Consumer Protection）、競争局（Bureau of

125 関連するルールは、45 C.F.R. pts. 160, 162, 164 に規定されている。
126 45 C.F..R. Part 164 Subpart E-Privacy of Individually Identifiable Health Information
127 HIPPA Security Standards for the Protection of Electric Personal Health Information, 45 C.F.R. Part 164
128 American Recovery and Reinvestment Act of 2009(ARRA)
129 The Health Information Technology for Economic and Clinical Health (HITECH) Act
130 Cable Communications Policy Act of 1984, Pub. L. No.98-549(1984)
131 Video Privacy Protection Act of 1988, Pub. L. No.100-618 (1988)
132 岡村＝新保　前掲 107　134 頁
133 Shaw・前掲注 61　67 頁
134 FTC による規制については石井　前掲注 95 408 頁
小向太郎「米国 FTC における消費者プライバシー政策の動向」情報通信政策レビュー第 8 号(2014 年)
135 Daniel J. Solove & Woodrow Hartzog, *The FTC and the New Common Law of Privacy* , COLUMBIA LAW REVIEW [Vol. 114:5839](2013)

Competition)、経済局（Bureau of Economics）の 3 つの部門がある。

FTC 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または欺瞞的な行為または慣行を、自然人、団体、または法人が行わないようにするための権限と責務を与えられている（FTC 法 5 条, 15 U.S.C. § 45(a)(2)）。FTC は、ビジョンを"A vibrant economy characterized by vigorous competition and consumer access to accurate information."[136] とし、「生産者が正確な情報を得た消費者を相手に活発な競争を行うこと、多様で高品質な製品が低価格で提供されること、効率性、革新と消費者の選択が促進されていること」を特徴とするアメリカ経済を肯定する価値観に基づいて、権限行使が行われる。また、FTC のミッションとしては「企業活動が反競争的、詐欺的または消費者に対して不公正であることを防止し、消費者の選択に関する情報と競争的過程に関する公の理解を拡大する」ことが掲げられているが、「正当な企業活動を不当に煩わせることなくこれを達成する」と付記されていることが、自由なビジネスによる経済の発展に高い価値を置く米国の立場を表している。

FTC の権限行使は、「不公正または欺瞞的な行為または慣行」に対して行われる。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または欺瞞的な行為または慣行は、違法であることがここに宣言される（15 U.S.C. § 45(a)(1).）」と規定している。ここでいう「不公正」とは「実質的な損害を消費者に与えるか与えそうなもので、消費者自身が合理的には避けることができないものであり、消費者や競争上の観点からの利点によって正当化されないものをいう（15 U.S.C. §. 45(n).）としている。これがキーワードとなる。

FTC の法執行には、行政的措置（Administrative Enforcement）と司法的措置（Judicial Enforcement）があり、行政的措置にはさらに「審決」と「ルール策定」の 2 つの手続きがある。日本の公正取引委員会も FTC に倣ったものである。

FTC は、法違反が生じていると「信じるにたる理由（reason to believe）」がある場合には、主張を訴状として発行することができる。訴状の対象となった者が FTC の主張を受け入れる場合には、同意審決（consent agreement）を結ぶことができる。対象者が FTC の主張に異議を唱える場合には、審判手続（Administrative Trials）に入る。委員会執行規則（Commission's Rules of Practice）に基づいて審判手続が行われ、審判官（administrative law judge ("ALJ")）によって判断されることになる。例えば、排除措置命令なども出すことができ、審判の 60 日後に発効する。一次審決に対しては異議申立が可能である。異議申立において、FTC は申立書と口頭での主張を受けたうえで、委員会としての最終的な決定と命令を発行する。FTC の最終決定は、連邦控訴裁判所に控訴できる。また、FTC は法的救済のために裁判所に予備的及び終局的差止命令を求めることができる。（司法的措置（Judicial Enforcement））。

セクトラルアプローチを取る米国では、1990 年代、情報ネットワーク社会の進展により新たな規範が必要になった時期も、制定法による個人情報保護よりも、BBB オンラインや Trust-e などの自主規制とその認証による信用の標章による顧客誘引、結果として信用できない事業者の市場からの退場、という形で個人情報保護を実現すべし、との意見が主流となった[137]。この背景には、1980 年代以降、福祉国家論の行き詰まりから世界的に進んだ規制緩和や市場

[136] FTC, "About the FTC" http://www.ftc.gov/about-ftc. （2017・6）

[137] インターネットにおけるプライバシー保護への業界団体のスタンスについては、岡村＝新保　前掲注 107　148 頁、第三者認証制度による自主規制については、同 135 頁

の力至上主義もあり、また、新たな技術やビジネスの発展を阻害しない、という理由もあった。

これらの認証では、個人情報の取扱についてのポリシーを公表することが義務付けられているため、消費者はポリシーを公表している事業者を信用する。やがて、認証を取らないにもかかわらず多くの事業者がこれを形式的に真似てプライバシーポリシーを公表するようになったが、実は実行していない、という例が出てきたため、FTC が欺瞞的商行為としてエンフォースし始め、実質的にプライバシー・セキュリティ分野での力を拡大してきた。上記の秩序枠組の中、その精神を踏まえた効果的な方法といえよう。

やがて、欧州からの個人情報移転制限に対応するために創設されたセーフハーバ協定において、欧州は規範の強制力を問題にしたが、セーフハーバの適用を申請する企業に一定のポリシーを公表させることによって、FTC のこの強制力を効かせる、という形で、自主規制を基礎としながらも強制力を持たせる枠組みを創出している[138]。

制定法上も、FTC に権限を与えるものが増え、FTC は具体的なガイドライン制定や強制などを行っている。例えば、前述した、1999 年の金融サービス近代化法は金融機関にプライバシー保護方針を明示することを義務付け、FTC に具体的な規定策定などの権限を与え、管轄当局のない事業者に対する強制も行っている。消費者の信用情報についても、1970 年、Fair Credit Reporting Act が制定され、消費者の信用情報レポート業者に対し、消費者の信用情報の機密性、正確性、適正利用の義務を定めたが、2003 年この後継となる Fair and Accurate Credit Transactions Act（FACTA）は更に、なりすましの防止を追加し、消費者は自分の信用情報を確認できるようになった。この法律に基づく権限に基づき、FTC は強制力あるガイドラインを出し、また、他の省庁が管轄しない「債権者」に対する強制も行っている[139]。また、子供の情報に関しては、1998 年 Children's Online Privacy Protection Act (COPPA[140])が制定され、13 才未満の子供の情報を Web サイトによる収集、使用、開示に対し、親の証明可能な同意が必要とされた。この法律についても、FTC が強制力を持っている。そして、テレマーケティングと消費者詐欺・悪用防止法（Telemarketing and Consumer Fraud and Abuse Prevention Act[141]）も FTC に権限を与え、FTC はこれに基づき Do-Not-Call を自ら運営し、強制も行っている。

これらのように、成文法に基づいて規則を制定している場合も多いが、そのほかにも、プライバシーやセキュリティに関する様々なガイドラインを公表している[142]。

2003 年からは、FTC の年次報告書でも、「Consumer Privacy」に独立した章が割かれるようになり、法執行と規則制定について、それぞれ独立した節で記述されている。そして、2012

---

138 岡村＝新保　前掲注 107　164 頁

139 Shaw, 前掲注 61　52 頁

140 15 U.S.C. §§6501-6506

141 15 U.S. Code § 6102

142 例えば、大きな指針として、FTC, Protecting Consumer Privacy in an Era of Rapid Change: Recommendations for Business and Policymakers, March 2012,を示している。これは、いわゆるパーソナルデータの取扱の三原則を示したものとして、知られている。18 頁。また、2012 年には顔認証ガイドラインを出している。FTC, Best Practices for Common Uses of Facial Recognition Technologies, October 2012　最近では、全米高速道路交通安全委員会と共に、自動運転と connected car についてのプライバシーとセキュリティに関するワークショップなども行っているが、やがて、ガイドライン化されるものと思われる。
https://www.ftc.gov/news-events/events-calendar/2017/06/connected-cars-privacy-security-issues-related-connected
(2017･7･16)

年以降は、FTC による取組のトップに「Consumer Privacy」が置かれるようになっている。

何よりも興味深いのは、それぞれの提訴事案における結論が、実質的に法規範を作っている面がある点である。まさに、「プライバシー分野のコモンロー[143]」と言えるだろう。ただ、判例法とちがうところは、同意審決で終わることが多い点である。そして、その内容も規範を形成している面がある。そして同意審決違反は裁判所に提訴され、高額の罰金を取っている。

プライバシーポリシー違反を梃子に強制してきた FTC だが、やがて、privacy policy がないケースや、web サービスなどの設定にプライバシー上の問題があるケースで privacy policy のどの条文に違反するかが明確でないものについても、「プライバシーへの消費者の期待への違反（broken consumer expectations of privacy）」であり不公正として提訴するようになった[144]。

また、セキュリティ事故についても提訴している。Wyndham 事件では、プライバシーポリシーにおいて安全管理措置を講じると明言しているにもかかわらず、セキュリティ・ホールを放置し 3 回のハッキングにより、ペイメントカード情報が流出し、数百万ドルの詐欺による損失を生じた。また、ペイメントカード情報がロシアドメインのサイトに流出した。Wyndham は、FTC はセキュリティに関して、FTC 法第 5 条に基づく不公正な行為として規制する権限がないと主張したが、第 3 巡回区控訴裁判所は、広く権限あり、と認めた[145]。

2016 年には、FTC は、ASUS に対し、ルータにセキュリティ欠陥があり、クラウドも脆弱だとして、20 年間、ユーザへのソフトアップデートの通知等を実行する、というプログラムを約束させる同意審決を取っている。また、オラクルに対し、Java に ID/PW 窃取やフィッシングのマルウエアに使われるひどい脆弱性を放置したとして、ソフトのアップデートの継続を約束させることで和解させるなど、かなり範囲を拡大している[146]。

4.2 漏えいに対する損害賠償

事後的な損害賠償については、漏えい事故が起きると、訴訟大国である米国では、例のごとく弁護士が先導して集団訴訟が起こるので、さぞ高額の損害賠償が認められているのではないか、という印象があるが、実は、契約違反や不法行為に基づき損害賠償請求はできるが、損害の立証が難しい[147]。というのは、米国の損害賠償では、実際に発生した損害（actual loss）でなければ賠償請求できない、という法理があるため、不安だけでは認められない。前述の Wyndham 事件のように、クレジットカード情報が盗られて、経済的に被害が出た場合は、損害賠償が認められることになるが、宇治市の個人情報漏えい事件のような場合は、詐欺などの具体的被害がない限り損害賠償は認められないことになる[148]。

---

[143] 前掲注 135

[144] Shaw, 前掲注 61、44 頁　Cart Manager case を事例として挙げている。同社はオンラインショッピングカートの会社で、消費者への直接の言明もなかったため、ポリシー違反による欺瞞ではなく、「不公正」を理由に提訴した。

[145] FTC, *Third Circuit rules in FTC v. Wyndham case,* (August 25, 2015), https://www.ftc.gov/news-events/blogs/business-blog/2015/08/third-circuit-rules-ftc-v-wyndham-case

[146] FTC, Privacy & Data Security Update (2016), https://www.ftc.gov/reports/privacy-data-security-update-2016(2017/6)

[147] Shaw・前掲注 61　120, 124-126
佐藤智晶「個人情報の流出と損害賠償責任―欧米の事例を参考に―」判時 2336　133 頁

[148] 最近は、経済的被害がない段階での提訴において、ディスカバリー前に却下を認めた決定に対し、抗告審段階

裏返せば、実損がある場合には損害賠償が認められることになる。だから、米国では、漏えい事故が起こると、漏えいした事業者は情報主体に対しクレジットモニタリングサービス[149]を無償で提供することが多い。損害賠償の mitigation の目的があると思わる[150]。しかし、消費者が自ら費用を支払ってクレジットモニタリングサービスを購入した場合、その費用は、将来リスクが増加することに備えたものであるとして、漏えい事業者に請求することはできない[151]。米国流の情報流出保険では、補償額のカバーというよりも、事故が発生した時の対応代行サービスとその費用のカバーに特徴がある。

不法行為では、更に、economic loss doctrine があり、その物自体の損害は、不法行為ではなく、契約法でしか請求できず、拡大損害のみが不法行為で請求できるとする。この理論は、PL 法でできたもので、情報セキュリティ事故のケースでは当てはまるとする州と当てはまらない、とする州がある。

このように、損害賠償は認められていないが、判例法の国なので、原告の立論次第で変わる可能性も高い。また、大型の漏えい事故が起こると、弁護士主導で集団訴訟が起こるのが米国である。最終判決までいかずとも、大型の和解案件がいくつかある。（表 6　一人当たり金額は単純計算で算出）

表 6　米国の主な和解案件

和解日	会社名	情報	和解金総額（$）	流出数	1人あたり和解額($)
2013/2/6	CBS Systems Inc. has	医療及びその他個人情報	112,000,000	292,000	383.56
2013/10/4	Rock Country Minnesota	運転手の個人情報	2,000,000	4,000	500.00
2014/2/28	AvMed Inc	顧客個人情報	3,000,000	1,200,000	2.50
2014/3/20	Stanford Hosital & Clincs	患者記録	4,000,000	20,000	200.00
2014/4/23	Concentra Health service Inc. and QCA Health Plan Inc.	患者記録	2,000,000	NA	NA
2014/6/23	Parkview Health System Inc.	患者記録	800,000	8,000	100.00
2014/10/24	TerraCom Inc.and Yourtel America.inc	SS#,名前、住所、免許、その他センシティブ情報	10,000,000	300,000	33.33
2015/9/17	Comcast	名前、電話番号、住所	33,000,000	75,000	440.00
2015/11/12	COX　Communication	顧客個人情報	595,000	60	9916.67
2016/6/20	モルガンスタンレー	顧客アカウントデータ	1,000,001	73,000	13.70

このように、一人あたりの金額は、まちまちだが、COX を除き、必ずしも多額ではない。しかし、流出数が多いと訴額が大きくなり、弁護士にとって、弁護士費用が稼げる案件にな

で、実質的になりすましのリスクがある場合は、訴訟手続きに進むことができる、との判断も出始めており、変化がみられる。例えば、Chantal Attias, et.al v. Care First, No.16-7108 (D.C. Cir.Aug. 1, 2017) https://www.cadc.uscourts.gov/internet/opinions.nsf/D38E2807B2E5DA5E8525816F0050E8C5/$file/16-7108.pdf しかし、あくまでも、なりすましによる経済的損害であって、日本のように、プライバシー侵害に基づく慰謝料を対象とするものではない。

[149] クレジットモニタリングサービスについては、4.5.2 節で詳説

[150] NY の侵害通知フォームでも、クレジットモニタリングを提供したか否かを訊いている。図 **8** 参照

[151] Shaw・前掲注 61 125, Pisciotta v. Old National Bancorp, 499 F.3d 629, 639-40(7th Cir. 2007)

るため、訴訟は尽きない。そして、1.3 節の図 3 の①②の上流企業にとっては、和解金の他、訴訟対応の手間、弁護士費用等の大きな負担が発生する。

4.3 中流：データブローカー

米国では、連邦レベルで包括的な個人情報保護法がない環境の中、データブローカーという事業が成り立っている。欧州の個人情報保護指令を梃子にした個人情報保護の機運の高まりの中、FTC も何度か問題視し、2012 年[152]、2014 年[153]の 2 回に亘り、データブローカーの実態についての報告書を出している。2014 年報告書では、データブローカーに調査をかけ、回答のあった 9 社を取り上げその実態を説明している。全世界で 7 億人分のデータとほぼすべての米国消費者に関するデータを持つ会社や、ほぼすべての米国世帯の情報をマーケディングデータとして提供する会社、など、かなり大規模な情報を保有している。提供目的もマーケディングキャンペーンや詐欺取引の発見、身元確認など様々であり、ユーザも民間から政府機関までである。

数十年に亘り、消費者が知らないところでデータを売買し、取引実態がわからないことに、政府は懸念を示してきた。1970 年の Fair Credit Reporting Act(FCRA)により、consumer reporting agency による与信、雇用、保険、住居等の審査用のデータの提供はカバーされたが、マーケティングや他の目的については、法律がない。

彼らは、Do-not-call 対象になったデータを削除（少なくとも「商品」には入らないようにしている）しており、この報告書に対するコメントでも、長年の産業全体の倫理規範があったことを示唆していることから、堂々としたビジネスとして対応しており、日本の名簿販売事業者のような闇のイメージはないのかもしれない。FTC は報告書の中で、透明性と説明責任を求めているが、二度にわたって報告書を出しても新たな規制ができないことから、かなり社会的な支持か政治力があると思われる。もしかしたら、知らない人に情報を持たれていることについて、日本のような神経質な反応がない背景なのかもしれない。

4.4 FTC の執行状況

FTC が活発に執行していることは、既に述べたが、その執行状況を分析する。FTC は毎年、執行状況の年次報告[154] を出しており、ここでは、2015 年及び 2016 年についての年次報告書に基づき分析する。FTC は、執行のケースについては、以下の 6 分類で報告しており、それぞれの執行数は表 7 のとおりである。

表 7 FTC の執行状況

[152] FTC,前掲注 142、 Protecting Consumer Privacy in an Era of Rapid Change: Recommendations for Business and Policymakers

[153] FTC, DATA BROKER; A CALL FOR TRANSPARENCY AND ACCOUNTABILITY, May,2014

[154] FTC, Privacy & Data Security Update (2016), https://www.ftc.gov/reports/privacy-data-security-update-2016 （2017・7・1）

FTC, Privacy & Data Security Update (2015), https://www.ftc.gov/reports/privacy-data-security-update-2015 （2017･7･1)

	2016 年までの訴追数	2015 年訴追数(含む継続)	2016 年訴追数(含む継続)
<1>プライバシー一般（General Privacy）	40 件 +ｽﾊﾟﾑﾒｰﾙ･ｽﾊﾟｲｳｪｱ関連 130 件	11 件	11 件 (内 2 件継続)
<2>データセキュリティ（Data Security）	60 件以上	4 件	5 件 (内 1 件<1>と重複)
<3>ｸﾚｼﾞｯﾄﾚﾎﾟｰﾃｨﾝｸﾞと金融ﾌﾟﾗｲﾊﾞｼ（Credit reporting and Financial Privacy）	ｸﾚｼﾞｯﾄﾚﾎﾟｰﾃｨﾝｸﾞ 100 件以上 金融（GLB）: 30 件	2 件	1 件
<4> 国際執行（International enforcement）(ｾｰﾌﾊｰﾊﾞの虚偽表示)	39 件	判決 2 件 和解 13 件	1 件
<5>子供のプライバシー（Children's Privacy）	20 件以上	2 件	1 件 (<1>と重複)
<6>電話勧誘制限（Do Not Call）	127 件	9 件	8 件

これらを第 1.3 節図 3 の上流（①②）の事業者、中流(③)の事業者、下流（④）の事業者に当てはめて分析する。

まず、<1>プライバシー一般と<2>データセキュリティは、個別の事案によって違うので、個別に分析する。2015 年、2016 年の<1><2>のケースは以下の通りである。

表 8　プライバシー一般事案

	<1>　プライバシー一般
⑴	Craig Britten：リベンジポルノサイトと称して、有償で削除する別のサイトに誘導
⑵	Jerk：悪口サイト（人を名指しし、悪口を書く）運営者。有償で削除する別のサイトに誘導。実は「名指し」は運営者が勝手にフェースブックから取ってきたものだった。
⑶	Nomi Technology:スマホが無線 LAN を探す際に出す MAC アドレスを検知して、客の動きをトレースするサービスを店に提供。プライバシーポリシーに、「Nomi でも店でも OPT-OUT を受付ける」、と書いているが、店では受付けていないし、店が使っていれば通知する、としているが、実行していない。
⑷	Trust e ：毎年認証を更新、と書いているのに、更新していない
⑸	Payment MD: Patient Portal(支払い管理) Patient Health Report(有料、健康情報履歴管理）: 4 か所の機関から集めるような告知だが、多くの機関から機微な健康情報を収集
⑹	Seqyiua One: データブローカー。サラ金申込データを買い、詐欺師に販売
⑺	Bayview Solutions, Cornerstone:消費者の信用情報（portfolios of consumer debt ）のデータブローカー。支払いが滞った債務者の情報を借金取りに売る。会員制の Web で売買しようとしたが、アクセス制御なく、誰でもダウンロード可能に。
⑻	CWB services 等十数社：サラ金業者たち。オンラインサラ金の申込者に入力させた口座情報をオークション。また、主犯のサラ金業者、データブローカーから購入。消費者が承認してもいないサラ金貸付として入金し 2 週間ごとに「返済」を継続引落。本人の抗議にも「同意あり」と主張。対銀行も同様。
⑼	pairsys:tech 詐欺　老人をだまして口座情報などを提供させる
⑽	Click45support:tech 詐欺　IT 大手の代理店と偽り、ウィルス感染と脅して口座番号などを提供させる
⑾	Prized Mobile app:モバイルゲームのポイント獲得アプリと称してインストールさせ、実はバーチャルマネーを窃取
⑿	Ashley：（セキュリティ管理弱かった）有償の完全消去サービスなのに消去していなかった、サクラ女性による勧誘、
⒀	Turn:モバイル会社。クッキー削除でトレースを止められると告知するも、他にも identifier を入れてトレース

⑭	Gigats：採用応募者の事前スクリーニング目的として情報を集めたが、実は、中等教育後の学校や専門学校の潜在顧客発掘目的（目的外利用）
⑮	Practice　クラウドベースの健康記録会社:開示を告げずに出させた、医者についてのレビューを開示。結果、患者の個人情報や病状、治療内容などのセンシティブ情報も開示された
⑯	InMobi　SG　スマホ宣伝会社：騙して位置情報取得、位置による宣伝を出す。罰金、95 万ドル、網羅的ﾌﾟﾗｲﾊﾞｼﾌﾟﾛｸﾞﾗﾑ　で和解
⑰	Vulcum:ｹﾞｰﾑに位置情報取得。同意画面なく直接デバイスに入れる
⑱	Tachht：スパム。偽の痩せ製品サービス。ハックされたメールアカウントを使い、知人からのメール見せかけ
⑱	12 のアプリメーカ：Silverpush　TV 利用をモニターするソフト
⑲	Sequoaia:データブローカー。Payday loa n に申込んだ人の情報を詐欺師に販売、詐欺師が銀行口座とクレジットカードを盗聴

表 9　データセキュリティ事案

	<2>　データセキュリティ
(21)	Oracle: java SE 脆弱性修正命じる
(22)	Whndam Hotel:3 度のハッキングでクレジットカード情報、ロシアへ
(23)	Lifelock:2010 年同意審決違反。約束した情報セキュリティプログラムの証跡なし。なのに、遵守、と公表している
(24)	Morgan Stanley:訴え取下げ。自主的に、内部犯行にも対応した網羅的セキュリティ対策したので。
⑫	Ashley:ｾｷｭﾘﾃｨ対策がお粗末で、大量漏えい（ポリシーなし、合理的ｱｸｾｽｺﾝﾄﾛｰﾙなし、教育不十分、第三者のｻｰﾋﾞｽが合理的ｾｷｭﾘﾃｨ対策しているか知らず、ｾｷｭﾘﾃｨﾓﾆﾀﾘﾝｸﾞの方法もなかった。同意審決
(25)	LabMD(医療検査)：被験者医療情報不適正にシェア。→内部統制プログラム、被害者へ通知、
(26)	ASUS:ルータにセキュリティ欠陥、クラウドも脆弱→ユーザへのソフトアップデートの通知、20 年プログラム
(27)	Henry:歯医者のｵﾌｨｽﾏﾈｼﾞﾒﾝﾄｿﾌﾄ、暗号レベル嘘。25 万ドル罰金

これらのケースを図 3 の①～④に当てはめると表 10　(1)～(27)のようになる。

また、表 7 の分類の他の項目については、以下のとおり検討し、表 10<3><5><6>で示す；

<3> クレジットレポーティングと金融プライバシ：自分が提供した情報ではない信用情報について、金融業者が保有し、又は流通している内容の開示と訂正を求めるものであり、基本的に③流通事業者、④本人の知らない利用事業者を対象とする。

<4> 国際執行：虚偽の表示を信用して欧州から移転した、というケースなので、この分類の対象から除く。

<5> 子供のプライバシー：COPPA 違反で、13 歳以下の子供の情報を親の同意なく取得、なので上流の①直接取得事業者を対象としている。

<6> 電話勧誘制限：提供した覚えがない事業者からの電話勧誘なので、④を対象にしている。

また、詐欺関連、データブローカー関与、および①～④の分類には該当しないがセキュリティ上重要なソフトウエアの脆弱性という注目点についても件数を示す。

（1 事案について、複数ポイントでカウントしているため、合計は事案総数より多い。また、<6>の Do not call 関連は数が多いため、＋〇件、と分離して表示）

表 10　2015 年～2016 年の FTC 執行事案の対象別分類と件数

対象	件数	ケース	例
①本人から取得する事業者	10 件	(1)(8)(9)(10)(12)(14)(15)<5>	目的外流用、騙して取得、削除義務違反、勝手に開示
①'アプリ等による不正取得、トレース	6 件	(3)(11)(13)(16)(17)(19)	アプリによる無断取得、騙して位置情報取得、実質的に OPT-OUT のないトレース
②直接取得事業者の安全管理	4 件	(22)(23)(24)(12)	
③　本人の知らない流通、提供、	8 件	(6)(7)(8)(19)(25)<3>	口座情報、借金多い人の情報の流通、詐欺師への売却
④　本人の知らない者による取得、利用	9 件 +17 件	(1)(2)(5)(8)(14)(19)<3> <6>	FB から勝手に web に。ﾌﾞﾛｰｶｰから買って詐欺に利用、
③、④の安全管理	1 件	(7)	
詐欺関連	8 件 +10 件	(1)(2)(6)(8)(9)(10)(11)(14)<6>の一部	Web から削除してほしければ金を払え 口座情報を入手して返済と称して継続引落 登録電話番号に詐欺目的で電話
データブローカー	4 件	(6)(7)(8)(19)	
ソフトの脆弱性対応	3 件	(21)(26)(27)	

このように、FTC は、②の取得した事業者の安全管理だけでなく、①の直接取得事業者による不正取得やアプリ等による無断でのトレースなど新しい問題も取り上げ、また、③の本人の知らない流通や提供、④の本人の知らない者による取得や利用についても、盛んに執行している。特に、詐欺が関係するものを優先的に調査している。消費者が損害を被る場合を優先する「結果ベースアプローチのプライバシー規制[155]」との考え方もあるかもしれない。また、前節で述べた通り 2012 年、2014 年にデータブローカーに関する問題提起をした直後のせいか、果敢にデータブローカーが関与した事案を取り上げ、詐欺グループとのつながりを暴いている。

4.5 FTC の検知力

通常の判例法では、当事者が損害賠償や差止を求めて提訴するため俎上に上りやすいが、FTC の提訴は行政調査であるため、現場のトラブルを発見する必要がある。トラブルが大きくなってマスコミに取り上げられたケースは発見が難しくないが、そうでないケースも取り上げているようである。どのように現場のトラブルを発見しているのでろうか。

4.5.1 通報しやすい仕組み

まず、FTC は、web サイトを通じ、なりすましや Do not call 違反を通報しやすい仕組みを用意している。

[155] J. Howard Beales III and Timothy J. Muris, *FTC Consumer Protection at 100: 1970s Redux or Protecting Markets to Protect Consumers?,* 83 GEO. WASH. L. REV. 2157, 2208 頁　消費者は、通常、プライバシー条項を交渉しないことから、メリットがありリスクを低減する個人情報の利用は歓迎されているのでこれを制限する必要はなく、消費者に害のある利用について規制なり提訴するのが生産的、という考え方。

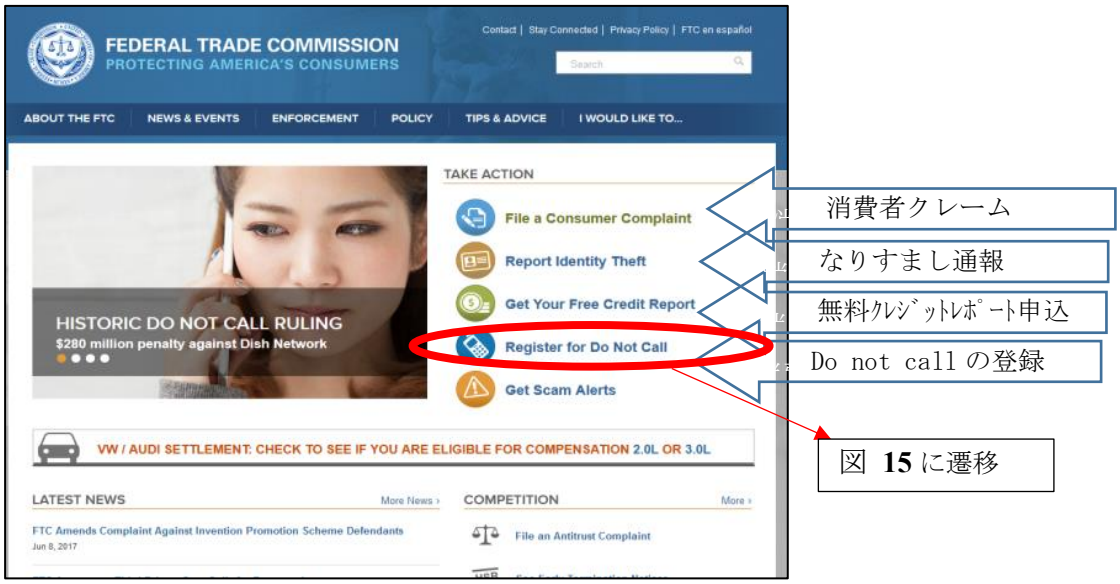


図 9　FTC トップページ（https://www.ftc.gov/）(2017･6･11 アクセス)

FTC のトップページ[156]に掲載されている項目は、①消費者クレーム、②なりすまし（Identity Theft）通報[157]、③無料のクレジットレポートの申込、④Do not call の登録・通報、⑤詐欺注意ニュースの申込となっている。②は、自分の情報を誰かが使っていることを発見して通報するものだが、④の Do not call も、自分が提供していないのに電話番号を事業者が持っていることも発見できる。②のクレジットレポートとは自分の信用情報を確認するものだが誰かが自分の名義で口座を開設したり借金をしたりしていることを検知することもできる[158]。つまり、②、③、④、は、自分の情報が知らないうちに使われていることを検知し通報することにつながっており、個人情報の不正利用・不正流通の発見につながる。

①消費者クレームのリンク先のページは図 10 の、for complaint assistance のページである。

156 https://www.ftc.gov/(2017･6･11)
左には、最近のニュースとして、Do not call 違反で史上最高額の罰金が裁判所で認められたニュースが大きく出ており、2017 年 6 月 6 日のプレスリリースにリンクしている。判決は、 U.S. v DISH NETWORK, C.D. Ill, No. 09-307 (June 5,2017) https://www.ftc.gov/system/files/documents/cases/dish_ilc_309cv3073_fact.pdf#page=451

157 FTC は、なりすましについては、別ドメインでも Web を立ち上げ、啓発と消費者が気楽に通報できる仕組みを用意して情報収集をしている。https://www.identitytheft.gov/

158 FTC はこのほかにも、モニタリングサービスについて啓発している。FTC, 「Identity theft protection services」 2016 年 3 月　https://www.consumer.ftc.gov/articles/0235-identity-theft-protection-services　(2017・4・1)

図 10　FTC　complaint assistant (2017･6･11)

左にカテゴリー別のバナーがある。上から①なりすまし（Identity Theft）通報、②詐欺・搾取（scam and rip-off)、③不要なテレマーケティング、メール、スパム(unwanted telemarketing, text or spam)、④携帯電話、電話（mobile device or telephones)、⑤インターネットサービス、オンラインショッピング、コンピュータ（Internet Services, Online Shopping, or Computers)、⑥教育、仕事、儲け話、(Education, Jobs, and Making Money）⑦クレジットと債務（Credit and Debt）⑧その他（others）となっており、通報・相談内容を整理しやすくしている。また、①、③が情報が使われていることに関係している。

また、上部の 2 つのアラートのうち、2 番目のものは、「事業者があなたの個人情報をどのように扱っているか心配ですか？プライバシーに関する心配を報告するにはここをクリックしてください。(concerned about how a company is handing your personal information? Click here to report privacy concerns.)」と、個人情報の取扱に関する報告を促している。また、ページの下部には、Do not call の登録や国際詐欺など、4 項目についての項目がある。

更に、FTC は、図 11 のとおり、なりすましに関するドメインももち、消費者がワンストップで相談できるようにしている。

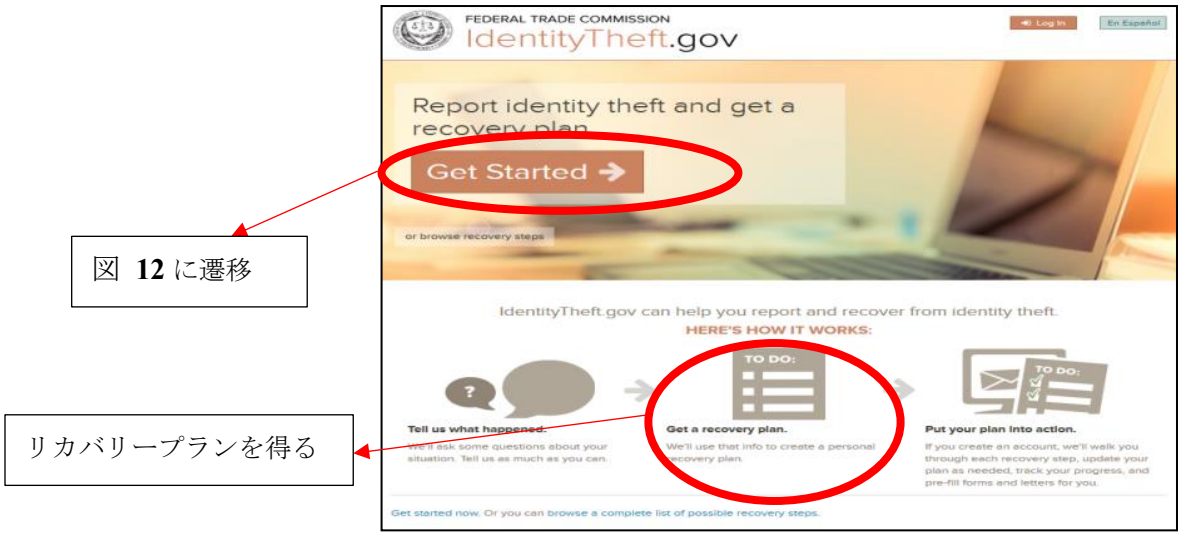


図 11　なりすまし通報ページ（https://www.identitytheft.gov/）（2017･5･7）

ページ下部にあるように、通報だけではなく、その消費者の自衛のためのリカバリープランの作成も支援している。

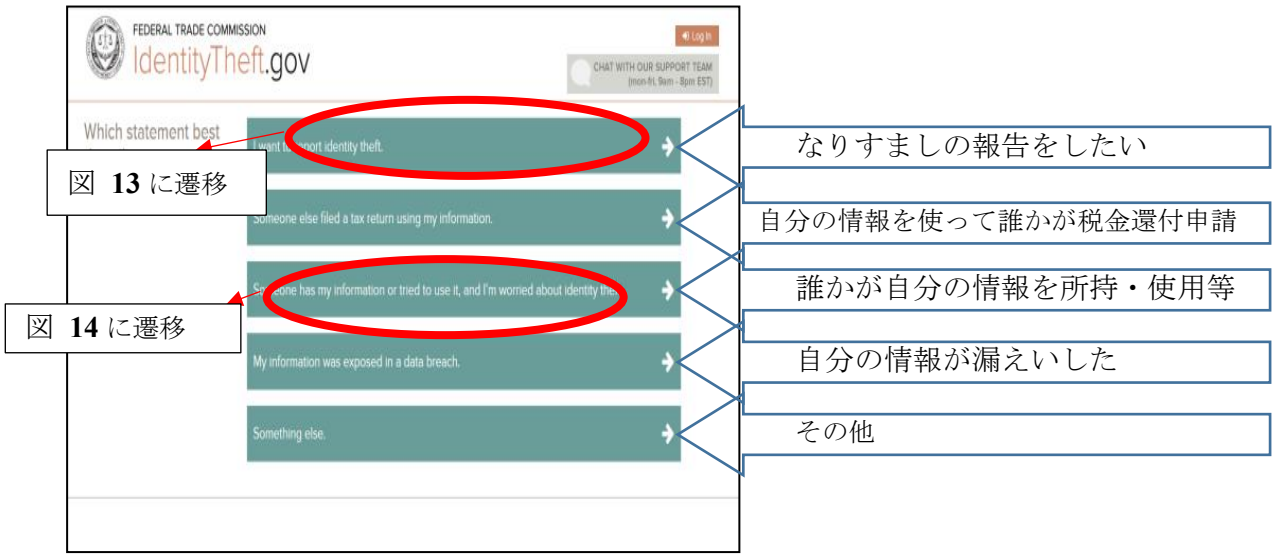


図 12　Get started のページ　(2017･6･11)

Get Started をクリックすると、図 12 のページとなる。ここでは、消費者が登録しやすいように、5 つのカテゴリーのバナーを用意している。

①なりすましの報告をしたい
②自分の情報を使って誰かが税金還付申請をした
③誰かが自分の情報を持っているか、使おうとしており、なりすましを心配している
④自分の情報が漏えいした
⑤その他

それぞれの内容にリンクすると、FTC が、消費者に具体的な被害が発生しそうな事案を特に取り上げていることがわかる。

例えば、①のなりすまし報告をクリックすると図 13 となる。

図 13　なりすまし報告ページ

ここでは、なりすまされた事項を選択するようになっており、①クレジットカード番号、②電話、携帯電話、ユーティリティ番号、③債務、当座・預金口座、④雇用、税金、⑤公的ベネフィット、ID、⑥ローン、リース、⑦他のアカウント（インターネット、保険、セキュリティ、医療等）と、選択できるようになっている。

図 12 の③の、「③誰かが自分の情報を持っているか、使おうとしており、なりすましを心配している」をクリックすると、図 14　となる。

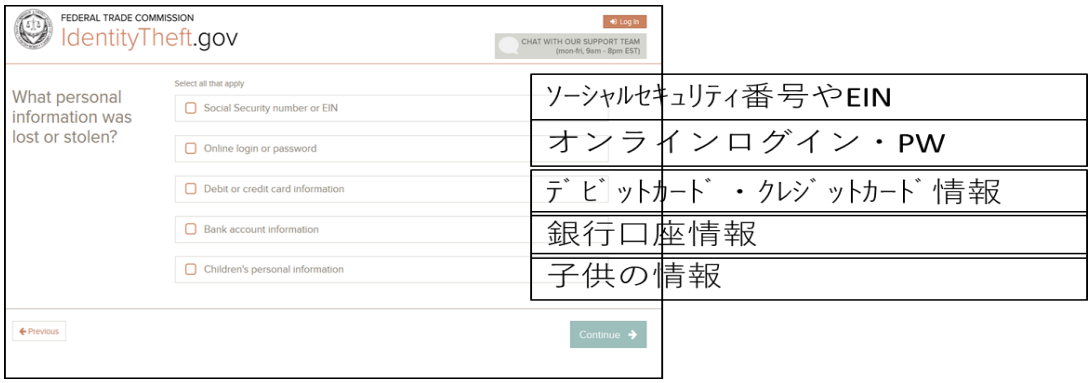


図 14　どんな情報が盗られたか？

そこでは、どんな個人情報が盗まれたか？を訊いている。選択肢として、①ソーシャルセキュリティ番号（社会保険番号）や EIN（Employer Identification Number）、②オンラインログイン・PW、③デビットカード、クレジットカード情報、④銀行口座情報、⑤子供の情報　があげられている。社会保険番号は、個人の身分証明としてよく使われ、EIN は米国の国税局にあたる IRS が発行している使用者としての ID で、日本の法人番号のようなものである

図 12 の「④自分の情報が漏えいした」をクリックすると、大量漏えい事件の典型的なものがリストされており、①Yahoo の漏えい、②IRS data retrieval tool for FAFSA（Free Application for Federal Student Aid (FAFSA) ）③OPM（office of personnel management）漏えい、④IRS の漏えい、⑤ここにはない、とリストされている。
②、③、④については、実際になりすまされたことがあるか、を訊き、なければ、一般的に気を付けることや、それぞれの機関が出している救済策、被害減少のための方策のページへのリンクとなっている。①や⑤については、具体的に使われた情報を訊くページにリンクしている。
また、図 9 の④Do not call の登録をクリックすると、図 15 のとおり、Do not call の登録や通報ができるページ[159]にリンクする。Do not call については、後述する。

図 15　Do not call　トップページ

このように、FTC は、消費者が通報しやすく、また、後日、通報内容を類型化して検索しやすいよう、通報サイトの項目に気を配っている。

4.5.2 クレジットモニタリングサービス

米国では、なりすましのモニタリングサービスがある。FTC は、消費者向け Web サイトで紹介もしている[160]。個人情報の漏えいやなりすましを防止するものではないが、例えば、クレジットカード番号が漏えいしていてなりすまして使われていることを早い段階で発見して被害の拡大を食い止めるものである。クレジットカードについては、日本でもクレジットカード会社が自衛と顧客サービスとしてそのようなことは行っているが、米国のこれらのサービスは、もう少し範囲が広く、情報主体が対価を払ってサービスを受けるものである。

159 https://www.donotcall.gov/
160 FTC, 「Identity theft protection services」
https://www.consumer.ftc.gov/articles/0235-identity-theft-protection-services (2017.4)

これには、クレジットモニタリングとなりすましモニタリングがある。

クレジットモニタリングは、サービスにもよるが、広くは下記のような場合に知らせてくれる；

- 誰かが信用履歴をチェック
- 情報主体の名前で新たなローンやクレジットカードが解説される
- 債権者や債権回収者が、情報主体の返済が遅れると言っている
- 公的記録上、情報主体が破産を申し仕立てたことになっている
- 情報主体宛に判決が出ている
- 情報主体の貸付限度額が変更された
- 氏名、住所、電話番号などの情報主体の個人情報が変更されている

また、なりすましモニタリングサービスは、銀行口座情報やソーシャルセキュリティ番号、運転免許書、パスポート、医療保険番号が、通常、情報主体の記録にはないような内容で使われていることをモニタリングする。サービスにもよるが、広くは下記のような所に情報主体の情報が出てくれば知らせてくれる；

- 住所変更届
- 裁判記録、逮捕記録
- 新たなユーティリティ、ケーブルテレビ、無線 LAN サービスの申込
- 給与担保ローン申請
- 小切手の現金化
- ソーシャルメディア
- 個人情報盗取犯たちが盗んだ個人情報を取引する Web サイト

料金は、1 か月、$10～$20 程度とのこと[161]。

これらのサービスにより、消費者は、対象となるような重要な個人情報の不正利用の発見を発見しやすくなり、FTC は、前述のような通報ページを介して、情報を集めることができる。

4.5.3 Consumer Sentinel Network

FTC は、これらの通報を受けて、すべてをすぐに自ら捜査することは不可能である。しかし、FTC は通報を他の執行機関と共有し、執行に繋げるしくみを持っている。

FTC は、1997 年、詐欺となりすましの苦情を集めるため、Consumer Sentinel Network (CSN)[162]を立ち上げた。これは、FTC が受けた苦情だけでなく、多くの州の検察や消費者法の執行機関、消費者金融保護局や国税局などの連邦の関連調査機関[163]や、the U.S. Postal Inspection Service, 民間の認証団体である the Better Business Bureau, Canada's PhoneBusters, the Identity

[161] ID 詐欺の恐怖 - クレジットモニタリングは意味があるか？2013 年 3 月 21 日
http://smartandresponsible.com/blog/credit-monitoring/ (2017.4)

[162] https://www.ftc.gov/enforcement/consumer-sentinel-network (2017･5･1)
FTC, THE FTC'S CONSUMER SENTINEL NETWORK
A FREE online investigative tool from the Federal Trade Commission,
https://www.ftc.gov/sites/default/files/attachments/consumer-sentinel-network/factsheet.pdf

[163] the U.S. Postal Inspection Service, the Identity Theft Assistance Center, Internet Crime Complaint Center, the National Fraud Information Center なども情報を提供している

Theft Assistance Center, Internet Crime Complaint Center,　the National Fraud Information Center などに寄せられた苦情が共有されている。なりすましだけでなく、ダイエット、債権回収等まで、幅広い消費者詐欺を対象としている。ここに、同様に FTC だけでなく、連邦、州、外国の法執行機関がアクセスでき、トレンドを見極め、悪質なケースを早く見つけ、証拠を集めている[164]。関連する法執行機関との協力や重複回避も行うことができる。ちょうど、日本における PIO-NET の大規模なもの、といえよう。

苦情は 5 年を経過すれば削除されるが、2016 年報告[165]によれば、現在データベースにあるのは 2012 年から 2016 年に寄せられた苦情で、約 13 百万件ある。このほかに、同期間に、20 百万件の Do not call の苦情が寄せられている、と付記されている。2016 年には、Do not call 以外で、3 百万件の苦情が寄せられている。FTC はそれを 30 カテゴリーに分けてデータベース化している。

詐欺のうち、負債回収にかかるものが 28%で最も多く、次が Impostor Scam (騙り詐欺。例えば、政府の人間を騙って、税金を払えとか、逮捕を免れるために金を払えとかいう詐欺の模様[166]。おれおれ詐欺、還付金詐欺もそのひとつ)で 13%、なりすまし（identity theft）13%、電話、携帯サービス 10%、銀行金貸し 5%と続く。

そして、消費者へのコンタクトの方法は、図 16 のように電話が 77%と最も多い。これは、Do not call が単なる消費者の迷惑防止のためだけではないことにつながっている。

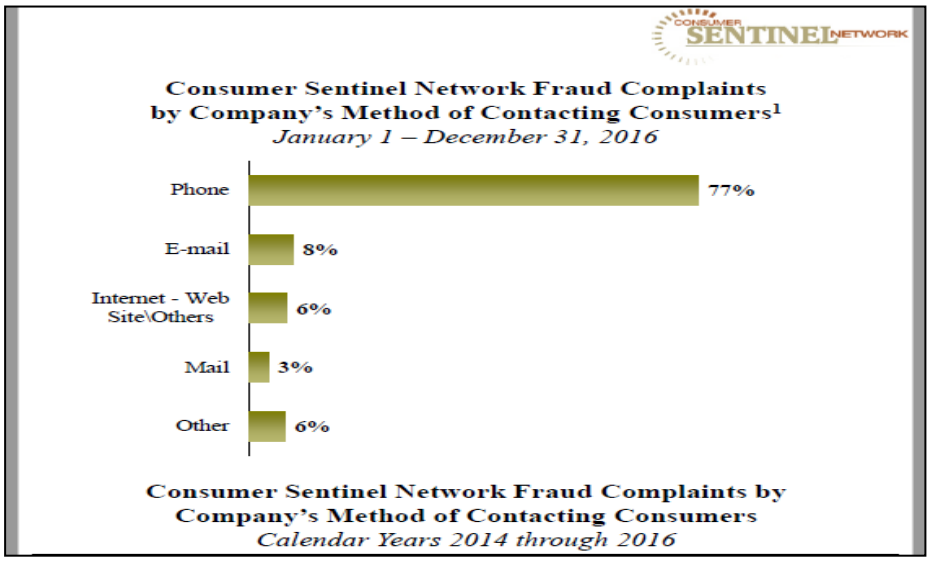


図 16　コンタクト方法

詐欺については、FTC だけでなく、検察も動きやすい領域であり、それぞれ、捜査、執行が行われる。このほか、FTC は、悪質なケースでの刑事訴追強化のため、詐欺被害者調査も

[164] Beales，前掲注 155、2177 頁
[165] FTC, Consumer Sentinel Network data book for Jan..-Dec. 2016, (Mar. 2017), https://www.ftc.gov/reports/consumer-sentinel-network-data-book-january-december-2016
[166] FTC, Scam Tag: Imposter https://www.consumer.ftc.gov/taxonomy/term/864

行い、これにより苦情が来なかったケースも含めた詐欺被害の大きさを示すことができ、捜査・刑事訴追強化のために、司法省刑事局とも連携している[167]。

このように、FTC は、消費者からの苦情を丁寧に集約し、連邦、州の法執行機関と対応している。1 件 1 件の苦情にすべて対応しているとは限らないが、統計的に見ることで、苦情の多い事業者には個人の感受性の違いを超えた客観的な問題があり、優先的に調査すべきと言え、合理的な方法であり、効率的な法執行の基礎となるものと考える。

なりすましは、経済的な被害もあり、詐欺につながる悪質な事案であり、優先的に調査することは合理的である。また、この犯罪への情報の使用を検知することで、そこから遡って、犯罪につながる個人情報の流通も調査が可能である。一般的な個人情報保護法がない中、データブローカーは、プライバシーポリシーも出さず、消費者との接点がないため「プライバシーへの消費者の期待への違反」を理由に FTC が提訴することも難しいが、悪質なものは、詐欺のほう助のような理由で、検察と共に調査することも可能になる。

また、このように苦情を集めて、調査事例を増やすことが、「プライバシー・コモンロー」のためにも重要なことである。理念先行で、世の中に指針を示すためのものや政治的なもの以外は執行が低調な国々よりも、地に足がついたものになる。更に、FTC 法 5 条に基づく判断となるため、理念先行型よりも合理的で現実を踏まえたものになる。4.1.3 節で述べたとおり、FTC のミッションには、「正当な企業活動を不当に煩わせることなくこれを達成する」と付記されており、自由なビジネスによる経済の発展に高い価値を置く米国の立場を表している。また、前述の Whydam のセキュリティ侵害による情報漏えい事件[168]で、第 3 巡回区控訴裁判所も、その判断において、「第５条は、とても精密とは言えないが、この条文が求めているのは、様々な関係する事実を考慮したコストベネフィット分析である」[169]、とし、「例えば、あるサイバーセキュリティのレベルにおける、消費者が被る合理的に避けがたい害（harms）の可能性と予想される大きさと、より強力なサイバーセキュリティ投資によって上昇する消費者のコストとの、コストベネフィット分析である」、としている。 「Wyndham が３回もハックされたことを考えると、裁判所は、最低でも２回目のハッキングで on notice があったと言え、Wyndham のサイバーセキュリティ実務は FTC 第５条のコストベネフィット分析を満たしていなかった、と判断できる。更に、FTC の非公式ガイダンスや、既に出ている同様のセキュリティ不足事案の提訴や同意審決により、FTC は忠告していた、ともいえる、」とした。ケースごとに現実的な合理的な判断をしつつ、後の事案における規範となるロジックを作っていく、いかにも判例法らしい理由づけだと考える。

[167] Beales, 前掲注 155、2178 頁
[168] Whyndham 前掲注 145
[169] 下線は、筆者追加

5　事故「実績」の日米比較

5.1 日本

日本では、日本ネットワークセキュリティ協会が毎年情報セキュリティインシデントに関する調査を公表している。これは、新聞やインターネットニュースの報道、事業者からリリースされたインシデントに関連した文書などをもとに、インシデントの情報を集計し、分析したもので、2005 年から継続して行われているため、価値の高いものである。

以下、同協会が公表している報告書の内、2016 年報告書と、簡単な経年変化を見るため、項目によっては、2014 年の状況の報告書[170]を参考にして分析する。

2016 年発生した漏えい件数は 468 件で、前年比微減。漏えい人数は、1,397 万人である。発生件数は、2014 年から減少している。漏えい人数は、2014 年はイレギュラな大量漏えい 1 件があったため、約 5000 万人となっているが、大量漏えい事件による漏えい人数 4858 万人を除いた 142 万人に比べれば、増加している（図 17）[171]。

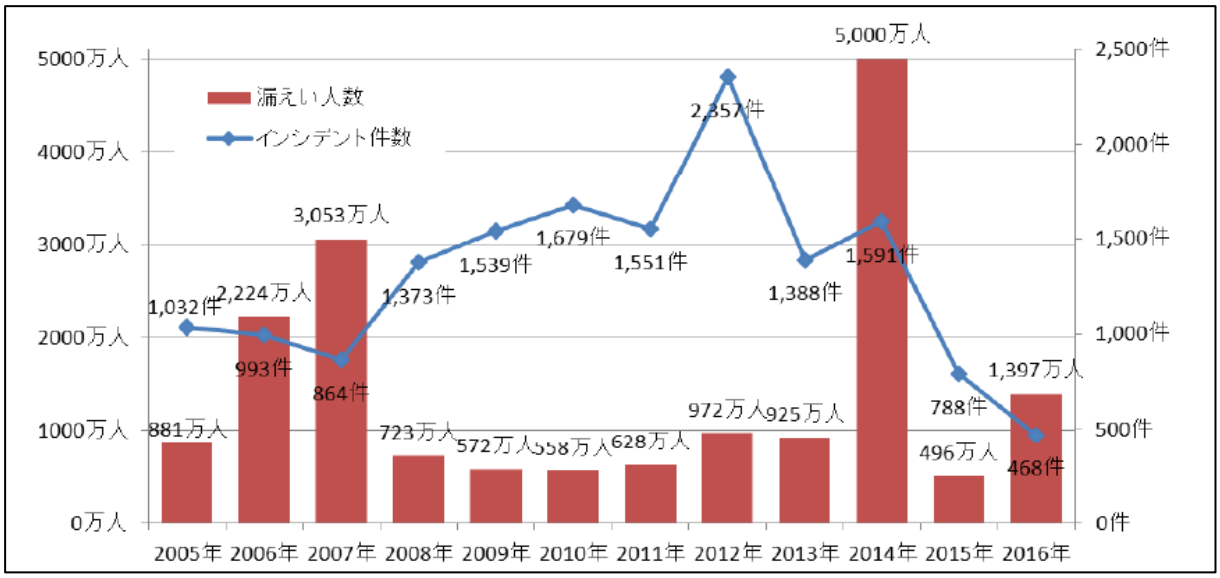


図 17　漏えい事件件数（折れ線グラフ）と漏えい人数（棒グラフ）

また、両年の規模の大きいインシデントトップ 10 は、表 11、表 12 の通りとなっている[172]。大人数の漏えいが発生しているのは、ウィルスや不正アクセスによるものが増えている。

---

[170] 日本ネットワークセキュリティ協会「2014 年 情報セキュリティインシデントに関する調査報告書　～個人情報漏えい編～」2016 年 7 月
http://www.jnsa.org/result/incident/2014.html
同協会日本ネットワークセキュリティ協会「2016 年 情報セキュリティインシデントに関する調査報告書　～個人情報漏えい編～」第 1.2 版　2017 年 6 月 14 日
http://www.jnsa.org/result/incident/data/2016incident_survey_ver1.2.pdf　(2017.6)

[171] 2016 年報告書　25 頁　図 4-29

[172] 2014 年報告書、4 頁　表 3-2、2016 年報告書、7 頁　表 4-2

表 11　2014 年度個人情報漏えいインシデントトップ 10

No.	漏えい人数	業種	原因
1	4858 万人	教育，学習支援業	内部犯罪・内部不正行為
2	16 万 4650 人	情報通信業	誤操作
3	13 万 1646 人	製造業	不正アクセス
4	9 万 4359 人	情報通信業	不正アクセス
5	6 万 1977 人	製造業	不正アクセス
6	5 万 6780 人	公務(他に分類されるものを除く)	誤操作
7	4 万 1477 人	公務(他に分類されるものを除く)	盗難
8	4 万人	金融業，保険業	管理ミス
9	4 万人	公務(他に分類されるものを除く)	内部犯罪・内部不正行為
10	3 万 9585 人	金融業，保険業	紛失・置忘れ

表 12　2016 年度個人情報漏えいインシデントトップ 10

No.	漏えい人数	業種	原因
1	679 万人	生活関連サービス業，娯楽業	ワーム・ウイルス
2	98 万人	情報通信業	不正アクセス
3	81 万人	電気・ガス・熱供給・水道業	紛失・置忘れ
4	64 万人	情報通信業	不正アクセス
5	58 万 9463 人	情報通信業	不正アクセス
6	42 万 8138 人	情報通信業	不正アクセス
7	42 万 1313 人	卸売業，小売業	不正アクセス
8	35 万人	生活関連サービス業，娯楽業	不正アクセス
9	21 万 9025 人	卸売業，小売業	不正アクセス
10	21 万人	電気・ガス・熱供給・水道業	管理ミス

漏えい経路別推移は件数ベースでは、図 18 のとおりである[173]。件数は激減しているが、件数としては紙媒体が多い。USB 等の媒体経由も微減。一方、不正アクセスなどインターネット経由のものが 2014 年に比べれば微増となっている。

[173] 2016 年報告書、2 頁　表 1-2

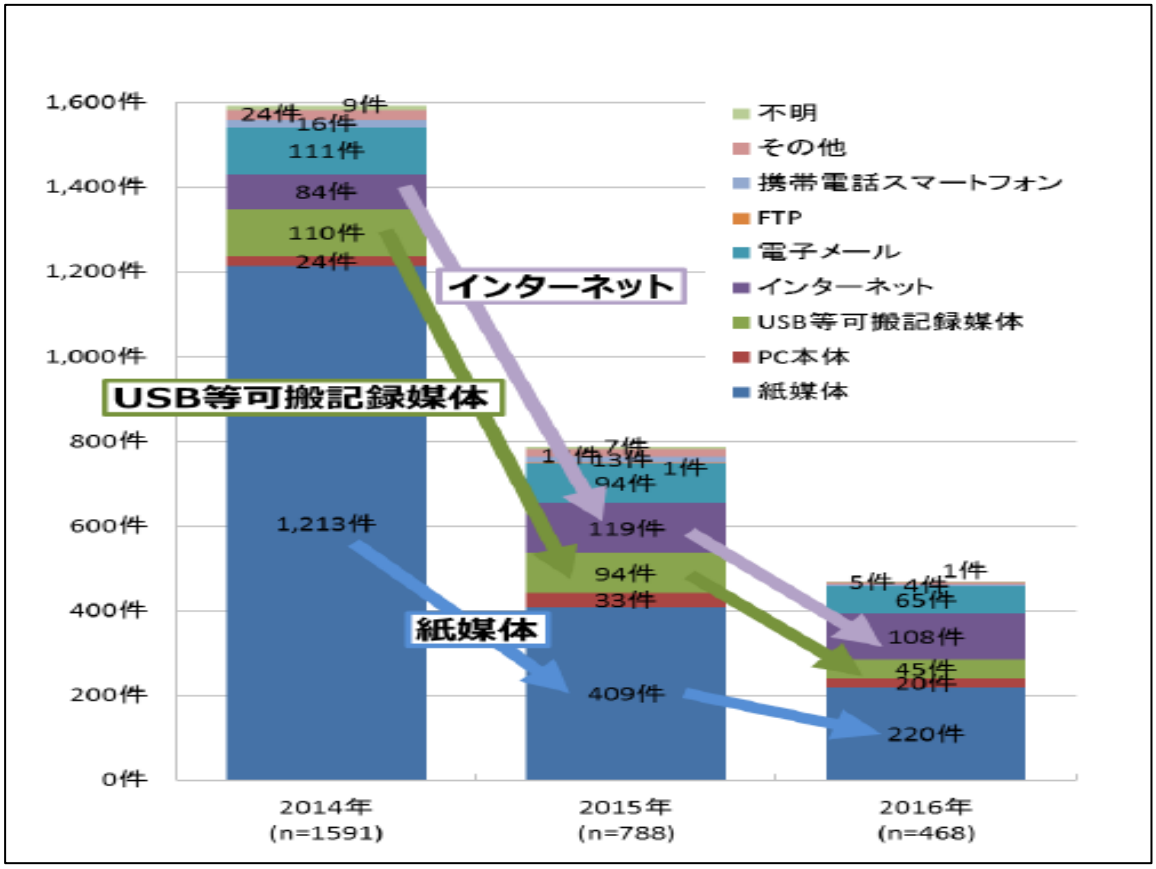


図 18 漏えい経路別インシデント件数

原因別事案件数推移は、図 19 のとおりである[174]。
不正アクセスが増加しているが、管理ミス、誤操作、紛失・置忘れが比率としてはまだ多い。

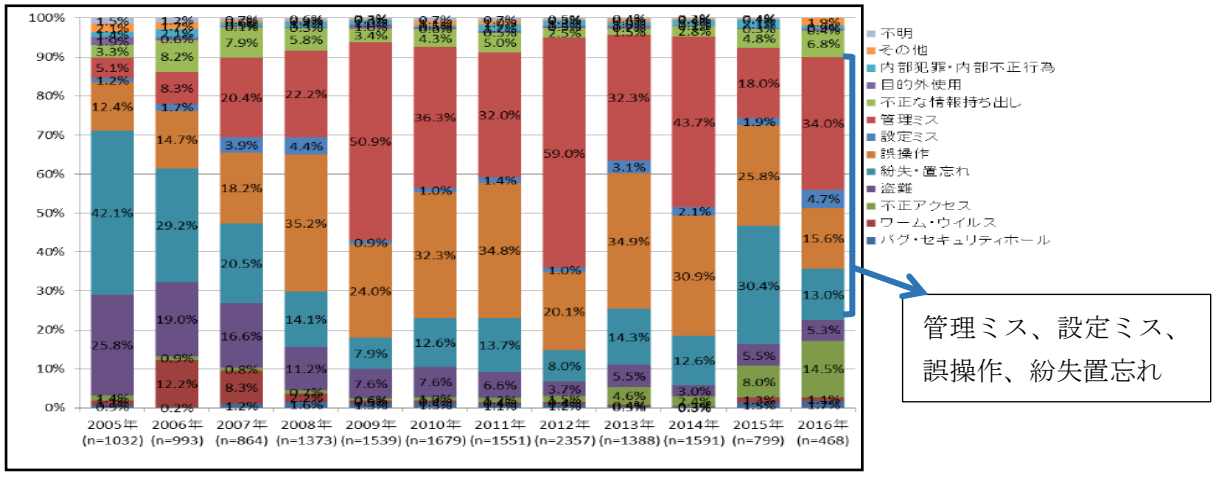


図 19　漏えい原因比率の経年変化(件数)

[174] 2016 年報告書、12 頁　表 4-9

2014 年と 2016 年の原因別漏えいの件数と人数では、図 20～図 23 の通りである[175]。なお、2014 年は、大規模なインシデント 1 件を除いたものである。漏えい人数は、ワーム・ウィルスと不正アクセスによるものが急増している。

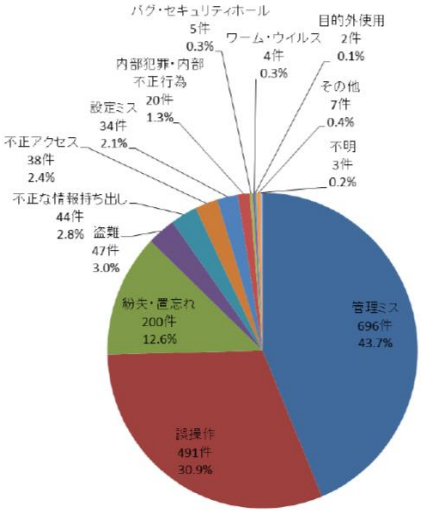


図 20　2014 年原因別件数と比率

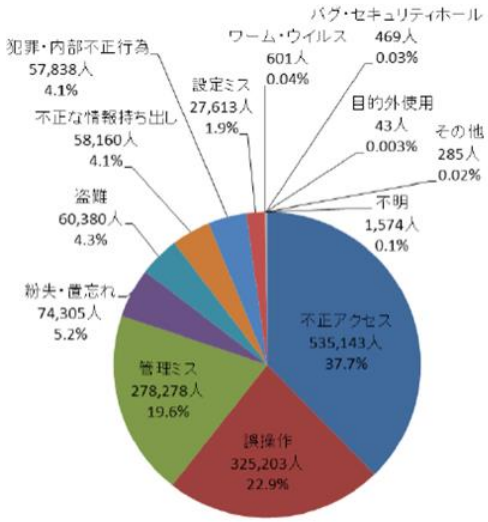


図 21　2014 年原因別漏えい人数と比率
(大規模なインシデント 1 件を除く)

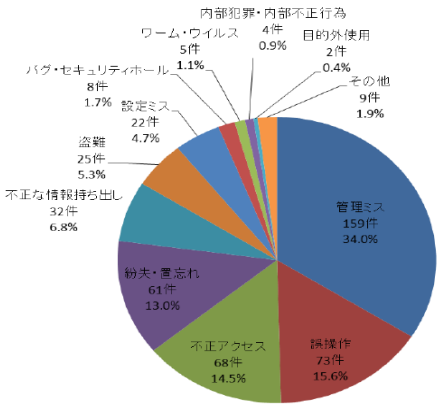


図 22　2016 年原因別件数と比率

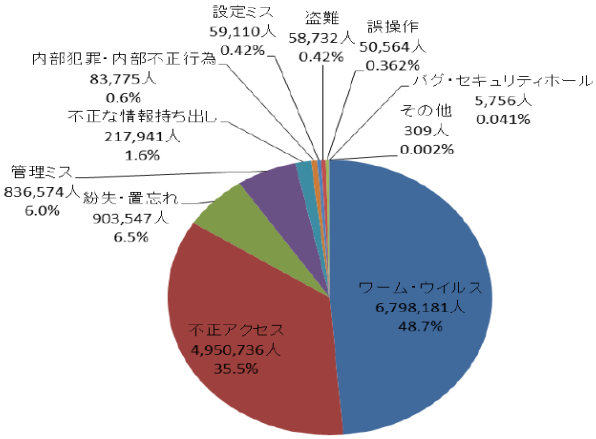


図 23　2016 年原因別漏えい人数と比率

また、2016 年度、個人情報の漏えい人数の原因別の一件あたりの漏えい人数は、図 24 のとおりである[176]。

---

[175] 2014 年報告書、15 頁図 3-11 漏えい原因比率（件数)、18 頁　図 3-14　「大規模なインシデント 1 件を除いた個人情報漏えい人数原因比率」
2016 年報告書、12 頁図 4-8 漏えい原因比率(件数)、13 頁　図 4-10 漏えい原因比率(人数)

[176] 2016 年報告書　1３頁　図 4-11

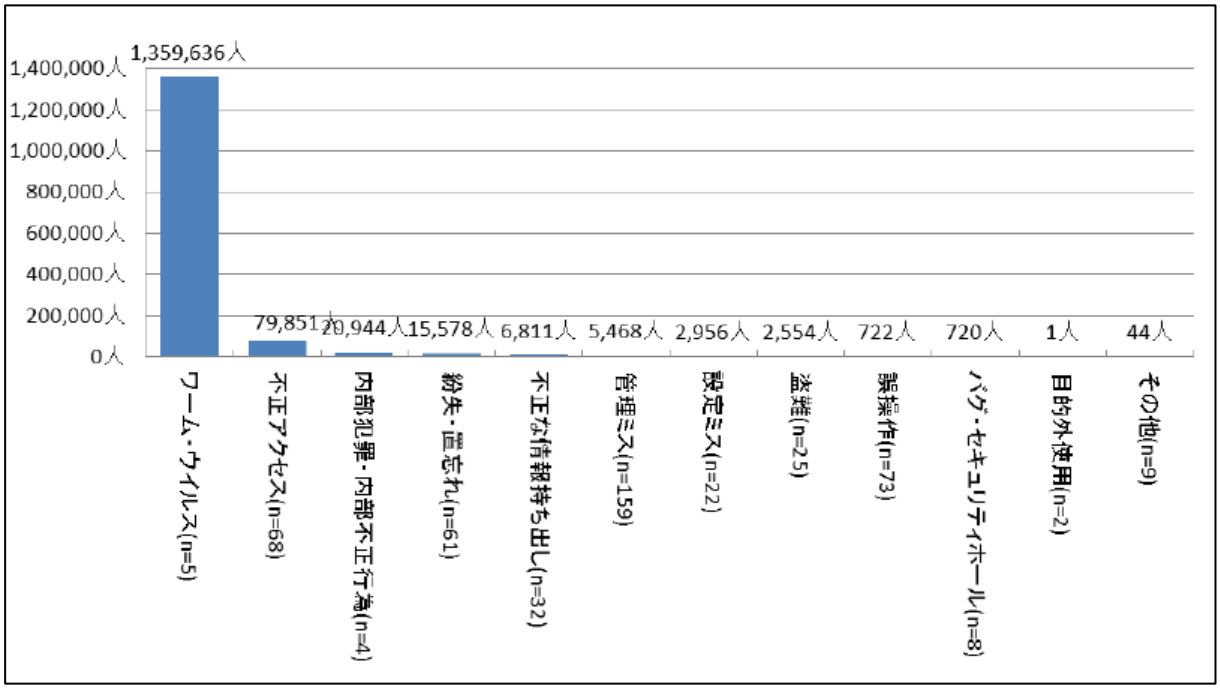


図 24　2016 年　漏えい原因別の一件当たりの漏えい人数

件数は管理ミス、誤操作、が多いが、1 件当たりの漏えい人数は、標的型攻撃とみられるワーム・ウィルスが最も多く、次に不正アクセス、内部犯行となっている。

5.2 ニューヨーク州

前述のとおり、米国ではほとんどの州に Breach Notification 法がある。ここでは、なりすましのリスクのある、ソーシャルセキュリティ番号、運転免許証等や経済的リスクのあるクレジット番号等が氏名と共に漏えいした場合に限定されるが、情報主体への通知と州当局への報告を義務付けている。

2016 年、NY 州検察が報告を受理したインシデント数は、1282 件で、漏えいのべ人数は約 160 万人で、過去最高であった[177]。

原因別では、表 13 のとおりである。やはり外部からのシステム侵害が最も多い。ワーム、ウィルスの項目がないので、不正アクセスとワーム・ウィルスを含むものと考えられる。

[177] ニューヨーク州検察,「A.G. Schneiderman Announces Record Number Of Data Breach Notices For 2016」,2017 年 3 月 27 日 https://ag.ny.gov/press-release/ag-schneiderman-announces-record-number-data-breach-notices-2016 （2017.4）

表 13　原因別個人情報漏えい状況

Data Security Breach Cause	Number of Breaches (% of Total)	NY Personal Records Exposed (% of Total)
External systems breach	519 (40.48%)	1,102,258 (69.05%)
Inadvertent disclosure	312 (24.34%)	304,277 (19.06%)
Other (i.e. skimming)	180 (14.04%)	50,313 (3.15%)
Insider wrongdoing	105 (8.19%)	7,300 (0.46%)
Loss of device or media	61 (4.76%)	9,607 (0.60%)
Merchant breach	38 (2.96%)	35,930 (2.25%)
Theft of device or media	19 (1.48%)	3,270 (0.20%)
Law enforcement recovery	18 (1.40%)	6,468 (0.41%)
Unauthorized access	13 (1.01%)	68,839 (4.31%)
Internal systems breach	10 (0.78%)	7,453 (0.47%)
Unknown	7 (0.55%)	492 (0.03%)
Total	**1,282**	**1,596,207**

これに基づき、1 件当たりの件数を計算すると以下の通りである。

表 14　NY 州　原因別 1 件あたり漏えい人数

	件数	人数	1 件当たり人数
外部からのシステム侵害	519	1,102,258	2123.8
不注意	312	304,277	975.2
他	180	50,313	279.5
内部犯行	105	7,300	69.5
デバイス媒体の紛失	61	6,907	113.2
merchant breach	38	35,930	945.5
デバイス媒体の盗難	19	3,270	172.1
法執行によるリカバリ	18	6,468	359.3
許可されないアクセス	13	68,839	5295.3
内部のシステム侵害	10	7,453	745.3
不明	7	492	70.3

1 件あたりの人数は、許可されないアクセスが最も多く、次に外部からのシステム侵害である。不注意が第 3 位、merchant data breach は、銀行ではなく、ユーザ企業での ID 乗っ取り等

による預金の引き出しという意味[178]と思われるが、これによるものが僅差で第 4 位である。

5.3 比較（ラフな分析の試み）

日本と NY で、原因別で、件数と 1 件当たりの漏えい人数を比較する。

両データは前提がかなり違うデータであり、乱暴な試みだが、試みに分析してみた。

基本は、2016 年比較で、日本は件数は図 22、人数は図 23 を、NY は表 14 のデータを使用した。また、参考までに日本は 2014 年についても、の図 20 から大規模な漏えい 1 件を除いた件数と図 21 の人数から比較した。

前提が異なる点は、以下の通りである。

① 人口：日本は 12000 万人、NY 州は 1980 万人

② 日本は、個人情報全部だが、報告義務はなく、公開されたものやリリース、報道を苦労して集めた結果であり、NY は、身分証明や金銭的被害に関係する情報と共に氏名が流出したものに限られるが、法律上の報告義務に基づき報告されたものである。

③ 原因の分類

これらの前提では、科学的比較とは言えないが、大まかな傾向は見つけられるかもしれないため、試みた。

まず、①、②については、分析にあたり、考慮することにした。

③について、比較の基礎となる、原因分類である。NY と日本で原因分類が異なるため、仮に下記の通り、分析用項目を置いた。

表 15 分析用原因分類項目

分析用分類	NY	JPN
外部不正アクセス	外部からの不正アクセス	不正アクセス
	merchant breach	ワーム・ウィルス
内部犯行・内部不正行為	内部犯行	内部犯行・内部不正行為
	許可されないアクセス	不正な情報持出
紛失、置き忘れ	デバイス媒体の紛失	紛失、置き忘れ
盗難	デバイス媒体の盗難	盗難
内部のシステム障害	内部のシステム侵害	バグ・セキュリティホール
不注意、ミス	不注意	管理ミス
		誤操作
		設定ミス
その他	他	目的外使用
	法執行によるリカバリ	その他
不明	不明	不明

次に、原因別 1 件当たりの漏えい人数を比較する。この分類に基づき比較を可能とするた

[178] 一説には、不正アクセスによる POS からのクレジットカード番号窃取と解する人もいるが、要調査。いずれにせよ、分析においては、外部不正アクセス。

め、それぞれの地域の原因別 1 件当たりの漏えい人数については、図 **24** を使わず、原因分類別に、総漏えい人数を件数で除して改めて算出した。日本については、図 20 から図 23 の数字を、NY は表 14 の数字を用いた。

表 16　原因別件数と 1 件あたり漏えい人数の比較

	NY 報告 2016		JPN 公表 2016		JPN 公表 2014	
	重要情報 義務		全個人情報 推奨			
	件数	人数/件	件数	人数/件	件数	人数/件
外部からのシステム侵害	557	2,043	73	160,944	42	12,756
内部犯行・内部不正行為	118	645	36	8,381	63	1,841
紛失、置き忘れ	61	113	61	14,812	200	372
盗難	19	172	25	2,349	47	1,285
内部のシステム障害	10	745	8	720	5	94
不注意、ミス	312	975	254	3,725	1,221	517
その他	198	287	11	28	9	36
不明	7	70	0	NA	3	525
合計	1,282		468		1,590	0

前提が仮説ばかりで、しかも基礎となる事業者数の比較がない状態で、乱暴な分析だが、試みに分析してみる。

まず、外部からのシステム侵害の件数に大きな差がある。日本は、2016 年には 2014 年から倍増してはいるが、NY に比べればまだかなり少ない。人口は日本はＮＹの 6 倍であること、対象となる個人情報の種類が NY では限られていることを考えると、日本における不正アクセスは少なすぎる。内部犯行についても、外部不正アクセスほどの差ではないにしても、日本は少ない。日本で公表が義務付けられていないためかとも考えられるが、2014 年の不注意、ミスや置忘れの件数はＮＹの 4 倍となっており、積極的に公表しているようにも見えるので、それが理由ではないと考えられる。日本は対策が進んでいるからなのかもしれないが、外部からのシステム侵害と内部犯行の 2 つは、内外の意図を持った者による犯行であり、組織として気付きにくいものなので、インシデント発生に気づいていないからかではなかろうか。

次に、紛失置忘れや不注意、ミスは、2014 年は日本の方がはるかに多かった。これらは、発生したら組織として気づきやすい類型であること、NY と違って個人情報の種類を問わずインシデントを公表していることにも関係するかもしれない。興味深いことに、2016 年には NY と同レベルの件数になっている。この分類の 1 件当たり人数が NY で少ないのは、重要性の高い個人情報なので、大量には持ち歩かないからかもしれない。

以上の日米の比較から、日本は、気づきやすい紛失等のインシデントは懸命に公表してきたが、気づきにくい不正アクセスや内部犯行を発見することができずにいる、と推測される。

外部からのシステム侵害や内部犯行など、インシデント 1 件当たりの漏えい人数が多いが

気づきにくい原因による漏えいが発見されるパターンとしては、以下のようなものがある[179]。

① 事業者のログの監視や異常な兆候を発見した時の分析によって発見[180]
② JPCERT などの外部監視機関から指摘されて発見
③ 漏えいした情報が Web などに掲示され、SNS などでその事実が広がり発見[181]
④ 漏えいした情報の不正利用が SNS などで話題となり発見[182]
⑤ 漏えいした情報が流通し利用され、本人から事業者への問合せによって発見[183]
⑥ クレジットカード情報など、漏えいした情報が流通し悪用され、クレジット会社からの指摘で発見
⑦ 情報の買取を請求されて発見

特に⑤に関しては、本人がその事業者にしか提供していない情報であることを管理している場合や、事業者ごとに住所表記などを変えて管理している場合でないと、なかなか難しい。そうでない場合、同様の問合せの数が多くなると、そこから漏えいした蓋然性が増えてくるので、それからログなどを調査して本当に事業者から流出したのか、犯人は誰か、を割り出すことになる。しかし、きちんとログを取っている事業者でないとなかなか難しい。このような案件では、漏えいしてから時間も経っていることが多いため、ログも残っていない事業者も多いと思われる。

このような条件に日米の差があるかは別途調査が必要だが、4.5.2 節で述べたクレジットモニタリングサービスなど、不正な利用を発見する仕組みがあることも一因であろう。本人が不正利用を発見し、FTC に通報し、漏えい元がわかることもあるだろう。

---

179 このほか、発見の端緒については IPA 情報漏えい発生時の対応ポイント集　2012 年 9 月 3 日 第 3 版 https://www.ipa.go.jp/files/000002224.pdf (2017.4)

180 例えば GMO https://corp.gmo-pg.com/news_em/20170310.html?_ga=1.138582075.9091588.1493533610#em00 (2017.4)

181 例えば、TBC 漏えい事件

182 例えば、チケットぴあ http://corporate.pia.jp/news/files/security_incident20170425.pdf (2017.4)

183 例えば、ベネッセ事件。「本年 6 月下旬から、通信教育事業を行う IT 事業者からのダイレクトメールが、弊社お客様宛てに届き始め、お客様からのお問い合わせが急増しました。弊社のお客様リストに基づいて営業活動がなされている懸念があったため、調査を開始しました。」㈱ベネッセホールディングスプレスリリース 2014 年 7 月 9 日 http://www.benesse-hd.co.jp/ja/about/release_20140709.pdf (2017.2)

6　日米比較と不招請勧誘規制

6.1 日米比較

第 2 章から第 5 章までの検討を踏まえ、日米を比較する。

米国では、網羅的な個人情報保護法はないが、個人情報が重要な分野については、セクトラル方式で立法されている。また、各州では、経済的被害や詐欺被害などが予想されるなりすましにつながると思われる情報については、侵害通知法で本人への通知と当局への報告を義務付けている。経済的被害や詐欺被害などが予想されるなりすましにつながると思われる情報については、個人情報が使われていることを検知するサービスや、FTC への容易な報告により、検知力が高い。おそらくそれとも関係して、大量に漏えいするが漏えい事業者としては気づきにくい内外の故意による情報漏えいについても、日本に比べて当事者が知ることとなる確率は高い。執行は、FTC や連邦・州の検察、当局などが情報を共有して行っている。また、漏えいを起こした図 **3** 上流の企業への損害賠償請求は、具体的な損害がなければ、最終判決としては損害が認定されないが、漏えい件数が大きければ、弁護士主導で和解狙いでも提訴するため、実質的には大きな負担となる。

このような米国の個人情報保護に関連する法の概観を表 17 に示す。

表 17　米国の個人情報保護法規範概観

	連邦	州
個人情報保護関連法又は関連条項がある成文法	対政府（プライバシー法） 対民間：セクトリアル ・金融、健康、子供等々	(対政府　) 侵害通知法
なりすまし詐欺消費者保護関連法	FTC法「不公正または欺瞞的な行為または慣行」に対応	（刑法）
訴訟：調査 判例法 (コモンロー）	「プライバシー・ コモンロー」 民事（契約法、不法行為法、等） (実損なければ損害無しだが、訴訟社会で和解多し）	

一方、日本では、理念に発する個人情報保護法とレピュテーションリスクとプライバシーマークにより、真面目な事業者・国民は、氏名と住所など、どのような個人情報についてもきっちり守ろうとする。しかし、萎縮効果も懸念されている。

また、プライバシーマークの審査も、日本人の神経質な管理に影響している。プライバシーマークは、歴史的には、日本企業にとって、品質保証の ISO9000 の次にポピュラーになっ

た認証である。当然ながら、品質保証の担当者は、PPM レベルの不良率を更に下げるために、きっちり管理することを叩きこまれた人たちで、それが日本の産業を支えた。しかし、ISO9000 の審査員の多くがこのバックグラウンドを持っていたため、日本における認証審査は他国に比べて厳しく、記録や形式にもこだわる伝統ができた。初期のプライバシーマークの審査では、この伝統を引き継いだ審査員も一定程度おり、規定の趣旨を踏まえた実態にあったやり方を認めず、認証にしか使わない詳細な書類を多く作成せざるを得なかった事業者も多い。これも、日本の個人情報保護に対する感覚に影響していると考える。

漏えい事故を起こした図 **3** 上流の企業への損害賠償も、ヤフー事件のように、個人の識別等を行うための基礎的な情報についても、「秘匿されるべき必要性が高いものではない」情報としながらも、本人が、自己が欲しない他者にはみだりにこれを開示されたくないと考えることは自然として、プライバシー侵害を認め、実損がなくても慰謝料を認めている。これは、漏えいによる不安だけでは損害がない、としている米国の状況とは全く違う。宇治市は法律に基づき地方公共団体に登録しなければならない情報を地方公共団体自身が管理不足のため漏えいした事件であり、ヤフーは電気通信事業者が漏えいした事件である。TBC は機微性の高い情報が流出し、ネット上に晒され、実際に、いたずら電話などの嫌がらせがあった事件である。また、それぞれ、個人情報保護法成立又は施行前の事件であり、裁判所としても、大きな規範の方向性を示すために、損害賠償を認めざるを得なかったケースともいえる。しかし、これが、日本において、基本 4 情報でもプライバシー侵害になる、として神経質になった原因の一つでもあろう。

個人情報保護法ができた時点で、不適正な取得・流通や不適正な利用は禁止されたはずであり、慰謝料の原因となるプライバシー情報の拡散や不安も減少したはずだった。しかし、その執行は、適正に取得したが事故を起こした事業者にのみ向けられ、名簿販売事業者の主務官庁も決められることなく、不適正な取得・流通や不適正な利用は野放しだった。

本来は、法律ができた時点で、金融や通信事業者でない民間の事業者による機微でない情報の漏えいで、従来と同様に考えるべきかどうか、同様に考えるとしても、せめて損害額について、検証が必要だったと思われるが、その後報道されているような訴訟はなく、現在に至るまで見直しはない。

推奨とされる侵害通知も、真面目な事業者は fax の誤送信や伝票の紛失のような少数のインシデントでも報告し、公表してきたが、事故隠しを批判されないレピュテーションを気にしない事業者には効いていない。細かな事故を報告してエネルギーを使う割には、発見が難しいが大量の情報が影響する外部不正アクセスや内部犯行など故意の窃取については、米国より検知力が低いか、兆しがあっても深く調査しないで目を瞑るのか、公表されていない。消費者が知らないうちに自分の情報が利用されていることを検知するサービスもない。真面目な事業者は神経質にエネルギーを使うが、レピュテーションを気にしない事業者による流通や利用は検知もされず、執行に向けた調査も低調である。

知らないところで流通していること自体はあきらめざるを得ない米国流の割り切りまで必要とは言わないが、もっと、合理的なシステムに変えることや、下流での検知力向上など、日本にも参考になることが多い。

これを、1.3 節図 **3** の①から④の当事者について表にまとめると、表 18 のようになる

表 18　日米の個人情報保護規範の「執行」状況

	米国			日本		
	①②取得者	③流通	④利用	①②取得者	③流通	④利用
個人情報保護法規	行政対象＋セクトラル			保護法（＋行政等＋条例）網羅的		
名簿屋規制	なし　FTC 報告が立法要請中			保護法上の条件満たせば合法		
侵害通知	重要情報について法的義務 州法＋一部業種			推奨　すべての個人情報		
実際	淡々と通知			二極化 些細な事故も対応／無対応 公表とﾚﾋﾟｭﾃｰｼｮﾝ		
執行	いずれも執行 消費者視点			上流の安全管理のみ執行 ﾚﾋﾟｭﾃｰｼｮﾝ		
検知力	故意犯行発見力？	？ 通報検知ｻｰﾋﾞｽ		故意犯行発見力弱い？	なし（苦情処理？）	
損害賠償	実損必要 多集団訴訟訟・和解			広くﾌﾟﾗｲﾊﾞｼ侵害 実損不要 訴訟がﾚﾋﾟｭﾃｰｼｮﾝ		

法も執行も、
なりすまし・詐欺に重点
流通、利用にも検知・執行

理念先行
知らない所で名前とコンタクト情報が流通していること自体が不安
しかし、検知なし
流通・利用への執行なし
規範上、収集者の安全管理のみで支える

日本においても、2015 年改正法を活用し、不適正流通や不適正利用に対する法執行が必要だが、その前提として、流通や利用を検知しなければ、調査が開始されない。しかし、経済的被害や詐欺被害などが予想される個人情報だけを対象とする検知や法執行だけでは、1.2.2 節で述べた日本における消費者の不安や、基本 4 情報の流通でプライバシー侵害になる日本の法制には応えることができない。個人情報を提供した覚えのない事業者から勧誘の電話がかかる、DM が来る、といった、不安にこたえるには、どうすればよいか。

ここで、FTC の運営しているような Do not call 制度が使える可能性がある。

6.2　米国の National Do not call　（DNC）

6.2.1 DNC　実体法

米国[184]では、まず、1991 年、電話消費者保護法（Telephone Consumer Protection Act[185]）に基づき FCC が規制してきた。そこでは、entity specific Do not call が導入され、住居の電話番号について、顧客から拒否されたときに、5 年間架電しないこと、そのための社内手続き文書を作成すること、但し、顕示的同意があれば架電可能なことが定められた。1994 年、Telemarketing and Consumer Fraud and Abuse Prevention Act[186](以下 TCFAPA という)により、一般的な消費者への脅迫、プライバシー侵害になる電話勧誘の規制権限を FTC に付与した。並行して、州法においても同様の対応が試みられた。

しかし、それでは、消費者は会社ごとに最低 1 回は電話を受けざるを得ず、テレマーケティングの発達で電話勧誘が増える中、不十分とされた。

2003 年、プライバシー保護及び消費者保護を目的として、Do-Not-Call Implementation Act が成立し、FTC 傘下に National Do not call Registry（全国迷惑電話お断り登録簿）が創設され、FCC に対して FTC との規制の統一化を命じた。

FTC による Do not call は、消費者保護領域という観点から、TCFAPA に基づき制定された Telemarketing Sales Rule[187](以下 TSR という)で定められている。

下記２種類の Do not call が「不正な電話マーケティング行為又は活動」とされ、違法とされている[188]

１）　顧客がその売主からの、又はその売主のための、電話マーケティングを受けたくない、と伝えたのにかけた場合[189]（以下 Entity-Specific Do-not-call という）

２）　顧客の電話番号が FTC が運営する、電話勧誘を受けたくない人の”Do-not-call”登録簿に登録されている場合[190]（以下 National Do-not-call という）

2003 年に導入された National Do not call では、消費者は National Registry にオンライン又はフリーダイヤルでの電話で電話番号だけを登録する。電話マーケティング業者は、業者登録すれば専用の Web サイトでこの登録簿にアクセスできる。アクセス料は、１エリアコードあたり、年間$60、全データにアクセスするためには、年間$16,482 となっている。電話マー

---

184 米国での DNC の導入の歴史及び法的課題の克服に関しては､佐々木秀智｢最近の判例　最近の判例 Mainstream Marketing Services, Inc. v. Federal Trade Commission, 358 F.3d 1228 (10th Cir.), cert. denied, 543 U.S. 812 (2004)--迷惑な商業テレマーケティングを規制する Do-Not-Call Registry は,プライバシーおよび消費者保護を目的とした,テレマーケティング業者の営利的表現の自由を必要以上に制約しない合理的な規制であり,合衆国憲法第 1 修正に違反しない」アメリカ法　2006(2), 365-371
アリス･ドラグーン「DO NOT CALL REGISTRY わずか 100 日で電話セールス撲滅システムを構築した米国連邦取引委員会」CIO : Business technology leadership 5(12), 90-99, 2004-12

185 Telephone Consumer Protection Act of 1991, 47 U.S.C. § 227 (the "TCPA")

186 15 U.S.C. 6101-6108　Do-Not-Call Implementation Act が 6102 に基づく TSR に規制。

187 16 C.F.R. Part 310

188 § 310.4.(b)(1)(iii)

189 § 310.4.(b)(1)(iii)(A)

190 § 310.4.(b)(1)(iii)(B)

ケティング業者が登録簿を確認せずに電話をすると TSR 違反になる。登録簿を確認し、30 日以内に自らの call list をアップデート、つまり、登録簿にある電話番号を削除しなければならない。[191]　違反に対しては、FTC、州検事、私人が裁判所で提訴が可能である。[192]また、違反者には、各違反につき 16,000 ドル以下の過料、全国での差し止め、等のペナルティがある[193]。

また、消費者保護と利用のバランスを取り、(i)その人が明確な書面で電話を受けることを同意したとき、(ii)その人とビジネス関係が確立し、Entity Specific Do-not-call の要請をしなかったとき、は、National Do-not-call 違反には、当たらない[194]。

しかし、電話マーケティング業者が登録簿を参照して自らの call list をアップデートする勧誘拒絶リスト取得型であり、業者は登録簿のデータをダウンロードが可能である[195]。このため、Do-not-call を順守するためにできたリストを他の目的に使用したり、販売、貸与、購入することも、「不正な電話マーケティング行為又は活動」とされている[196]。

この制度が導入されて間もなく、テレマーケティング事業者たちから、この制度は憲法で保障された言論の自由(営利的言論)を侵害し、テレマーケティング業界で雇用されている何十万という失業をもたらす、として、FTC に対する複数の訴訟が提起された[197]。第一審で FTC が敗訴し、一時、その運用の仮差し止めも認められたが、控訴審で連邦高裁は合憲と認め、最終判決として確定[198]した。日本と同様、米国でも営利的言論にも言論の自由が認められているが、思想信条に関する言論よりは、より公益とのバランスが問われている。この判決では、営利的言論への規制の判断基準である Central Hudson 判決基準に基づき、①当該規制によって達成される実質的な公益の存否、②規制がその政策を直接促進するか否か、③規制が必要以上に言論を制約しないように限定的に画定されているか、を判断した。①については、プライバシー、消費者保護目的として認められる。②と③について、他に考えられる選択肢を上げて検討した。具体的には、事業者による自主規制、Do not call のような消費者の自主的対応の法的支援、テレマーケティングなどの全面禁止の選択肢の中で検討し、自主規制では成果が上がらなかったこと、全面禁止は営利的言論への抑圧が過剰であることから、Do not call による規制を合憲と判断した。

この後、テレマーケターの中には、効率的な架電方法として、また、自ら電話番号を持たなくても総当たりで使われている電話を探す方法として、自動電話を導入し、使われている電話を特定する方法をとった者がいた。電話を受ける側から見れば、電話に出るといきなり切れるか事前に録音されているメッセージが流れることになり、迷惑な電話として、問題に

---

[191] FTC, *Complying with the Telemarketing Sales Rule,* "Protecting Consumers' Privacy", "Do Not Call Provisions", "The National Do Not Call Registry Requirements",
https://www.ftc.gov/tips-advice/business-center/guidance/complying-telemarketing-sales-rule (2016.9)

[192] FTC 前掲注 191" Who Can Enforce the Rule?"

[193] FTC 前掲注 191" Penalties for Violating the Rule"

[194] §310.4.(b)(1)(iii)(B)(*1*),(*2*)

[195] FTC 前掲注 191" Accessing the Registry"

[196] §310.4.(b)(2)

[197] ドラグーン・前掲注 184 によれば、アメリカン・テレサービス・アソシエーションとダイレクト・マーケティング・アソシエーションがそれぞれ提訴、とされている。

[198] Mainstream Marketing Services, Inc. v. Federal Trade Commission, 358 F.3d 1228 (10th Cir.), cert. denied, 543 U.S. 812 (2004)

なった。そこで、2008 年には、TSR が改訂され、録音メッセージにより人が介在することなく架電する自動電話（auto call、ロボコール）を事前同意なくかけることが禁止されている[199]。

6.2.2 DNC 強制手続きと実績

4.5 節で FTC の消費者クレームの検知を紹介したが、DNC においても、FTC は消費者が簡単に登録できるようにしている。

FTC の Do not call のトップページは図 15 に示したが、その画面の右側の「register you phone」から、すぐに図 25 の登録画面にリンクする。そこでは、登録する電話番号と連絡用の電子メールアドレスだけを登録する。

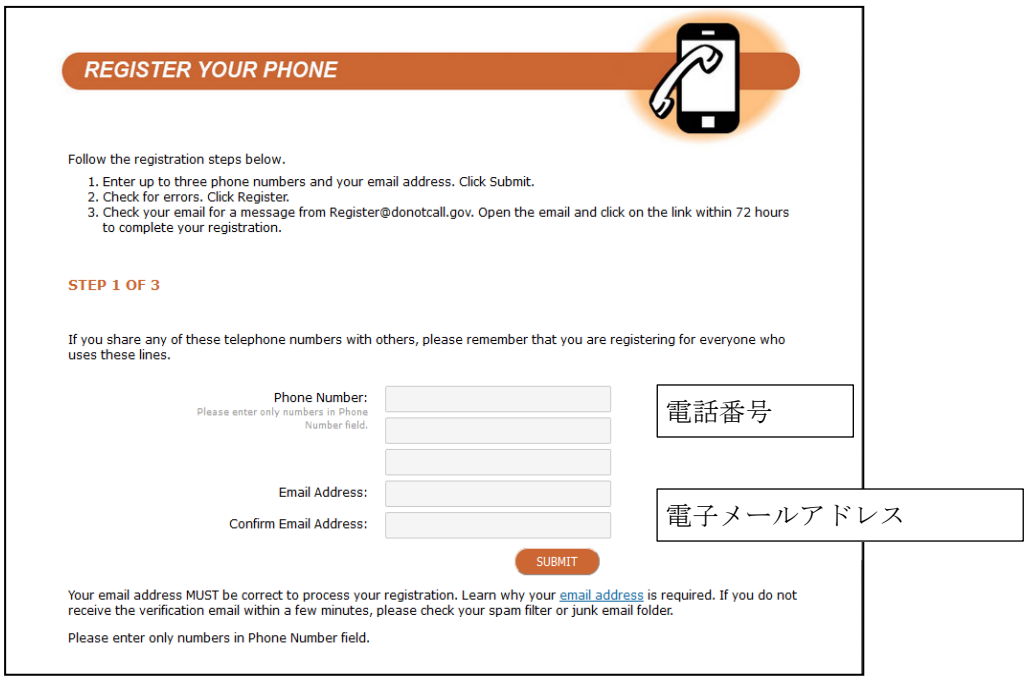


図 25 DNC 登録画面

また、通報については、図 15 の左側の「report unwanted call」から図 26 の通報画面にリンクする。

199 § 310.4(b)(1)(iv) 消費者が電話に出てから、2 秒以内に人が出ることを義務付けている。

図 26　DNC　通報画面　ステップ 1

そこで、電話番号、受信日時を記入し、ロボコールだったか、携帯電話にかかってきたかを選び、何に関する電話だったかをプルダウンメニューから選ぶ。

図 27　DNC　通報画面　ステップ 2

そこでは、わかる範囲で、電話をかけてきた者の電話番号、会社名を記入し、過去 3 か月以内にその会社と取引があったか、その会社に電話をかけないよう伝えたか、を選び、必須ではないが、FTC がコンタクトできる通報者の連絡先を記入する欄がある。記入は任意だが、そこには、「連絡先があると調査を進めやすい」、との説明がある。また、調査に役立つと思

われる追加情報を自由に記入できるコメント欄がある。

そして、「submit」をクリックすると、図 28 のような登録完了画面になる。

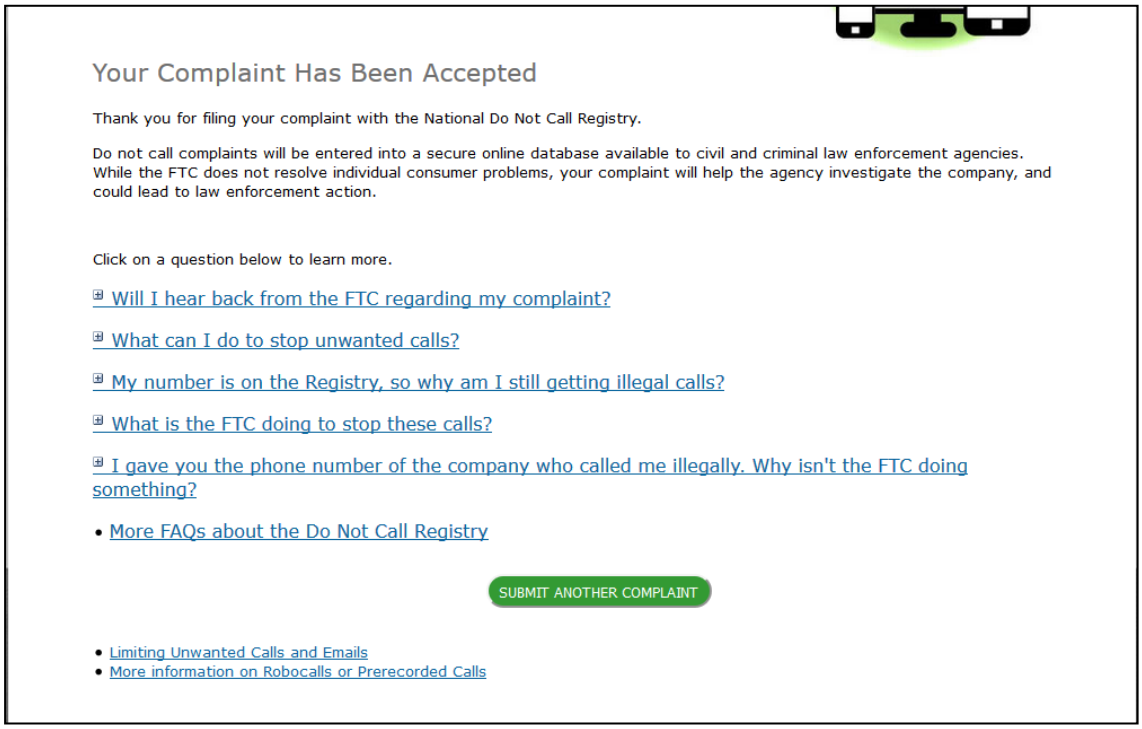


図 28　DNC　通報画面　登録完了

そこには、「Do not call の苦情は、民事・刑事の法執行機関がアクセスできるセキュアなオンラインデータベースに登録されます。FTC は個々の消費者のトラブルを解決する訳ではありませんが、あなたの苦情は、法執行機関がその会社を調査し、法執行につなげることができるかもしれません。」と、Consumer Sentinel の説明がある。

前述のとおり、DNC 違反については、FTC,FCC,州検察、私人が提訴可能である。

FTC 自身の執行手続きとしては、TSR の上位法である TCFAPA に基づく Telemarketing Rule で、違反に対しては、FTC が他の消費者保護事案と同様、「不公正・欺瞞的行為として扱う」、と定めて[200]おり、DNC に特別な手続きがあるわけではない。州検察による起訴においても裁判所において行われており、特別なものはない。FTC 自身が登録完了画面で説明しているように、個々のケースを全部調査するのではなく、苦情の多いものを調査している模様である。

開始した 2003 年の年末までに、消費者からの苦情は 15 万件に達し、100 以上のクレームが集中していた 45 のテレマーケティング事業者に対し FTC は提訴しており、例えば AT&T にすら、登録簿を無視したことで 78 万ドルの罰金を科している[201]。FTC や FCC の調査では、

[200] 15 U.S.C. 6102
(c) Violations
Any violation of any rule prescribed under subsection (a)—
(1) shall be treated as a violation of a rule under section 57a of this title regarding unfair or deceptive acts or practices;
[201] アリス・ドラグーン　前掲注 184　99 頁

しばしば内部是正プログラムを作成させ、政府が定期的に監査することを約束させることで和解している[202]。

FTC の 2016 年報告[203]によれば、2016 年 9 月末現在の登録者は 226,001,288 人で、前年より約 300 万人増加、1 年間で受理した苦情の数は 5,340,234 件となっている。約 2 万社のテレマーケティングを行う事業者が登録している。

4.4 節で述べたとおり、Privacy & Data Security update[204] では、FTC による執行案件を、①General Privacy、②Data Security、③Credit Reporting &Financial Privacy、④International Enforcement、⑤Children's Privacy、⑥Do not call に分けて、短い説明と共にリストしている。FTC が Do not call を"Privacy & Security"の一つのジャンルとして取り組んでいることがわかる。

Do not call では、2003 年以来提訴した事案は 127 件で 411 社 320 人を提訴している。勝訴した 118 件で合計 147 百万ドルの過料、10 億ドルの monetary restitution for victims(返還、補償), 不正利益返還の成果を上げている、と解説している。

2016 年の事案として 8 件があげられている[205]。

表 19　2016 年　Do not call 執行案件

・KFJ　Marketing:1.3M人のDNCRの番号に自動電話（DOJと共に連邦裁へ）	自動電話
・USA　10万件以上のVacation:DNCRに自動電話。BBBとFTCが接触後も。（和解）	自動電話
・Feature Films:117百万以上のTSR違反の欺瞞的違法な電話。（DOJが2011年にFTCのために提訴。裁判所で勝訴。陪審でDNCで勝訴した初のケース）	詐欺
・Life Management:自動電話。15.6百万円以上消費者からだまし取った（州検察と）	自動電話、詐欺
・Lanier法律事務所など（担保変更枠組み）：DNCRに電話。登録番号を入手する年会費不払い。	電話
Advatising Strategies:TROと仮差止。年金生活者から、詐欺的電話マーケティング。$9M被害、DNCRに電話、自動電話も含み、FTCActとTSR違反、	詐欺、自動電話
・Consumer Edu.：DNCRに2M件以上、自動電話含め。電話することの同意を入れずにWebで収集。（DOJと提訴、仮差止と過料）	自動電話、情報詐取
・国際自動電話一掃キャンペーン39件違法な自動電話を提訴（カナダ、UK,DOC<FCC,州検察と共同）	自動電話

[202] 例えば、*In re* Sprint Corporation f/k/a Sprint Nextel Corporation, (FCC, DA-14-527, May 16, 2014) https://apps.fcc.gov/edocs_public/attachmatch/DA-14-527A1.pdf

[203] https://www.ftc.gov/system/files/documents/reports/national-do-not-call-registry-data-book-fiscal-year-2016/dnc_data_book_fy_2016_post.pdf

[204] FTC・前掲注 146

[205] KFJ Marketing, LLC,、USA Vacation Station、Feature Films for Families, Inc., Life Management Services, Inc. Lanier Law LLC、Advertising Strategies, LLC, Consumer Education Group, multinational robocall sweep

2008 年の改正で TSR 違反となった自動電話に関する事案で苦情の多いものが目立つが、詐欺のための電話の事案も目立つ。例えば、Advertising Strategy のケースでは、退役軍人を含む年金生活者をターゲットに投資話を持ち掛けて金をとっているケースで、詐欺の立証があやふやでも、National Do Not Call Registry の電話への架電で有罪としている。Consumer Sentinel で、詐欺のコンタクト手段で電話が最も多かったが、Do not call はこのように消費者保護にも活用されている。

6.3 不招請勧誘規制

6.3.1 日本における不招請勧誘規制

日本では、1960 年代後半から 70 年代にかけて消費者問題が社会的に注目され、1976 年、「訪問販売等に関する法律」が成立した。主に訪問販売に関する規制ではあったが、一部、通信販売についても広告規制が入った。1990 年代に入り世界的にテレマーケティングが発達し、電話を利用した勧誘が急増した。そこで、1996 年、広告規制のみであった電話勧誘販売が、独立の取引形態として規定されることとなり、書面交付の義務化及びクーリング・オフ制度の導入等、訪問販売に類似した規制や、一旦断った消費者に対する再勧誘禁止が設けられた。また、この時、消費者が、行政機関に対して、調査及び措置を求める申出制度が設けられた。その後、インターネットの普及により、消費者がインターネットで商品を購入するインターネット取引が増加したが、その際、広告と契約手続との区別が不明確なサイトにおけるトラブルも出てきたため、2000 年改正では、通信販売においてインターネット販売を念頭に、顧客の意に反する申込みの禁止という広告規制が強化された。この時、消費者に対する多様な勧誘の規制を対象とするため、法律の名称が「特定商取引に関する法律」に変更された。

また、同じころ、電子メールによる広告を含んだいわゆる迷惑メールが送り付けられることが問題となり、2002 年 6 月改正で、電子メールによる勧誘広告のオプトアウト規制（広告の送付は原則として自由であるが、送信を拒否した者に対して広告を送信することを禁止した。）を導入した。当時の日本では、世界に先駆けた imode の発達により、携帯電話でのメール利用が普及しており、夜中のメール受信で目を覚ますというまさに迷惑メールだったわけだが、規制の対象は電子メール一般だった。その後、2008 年改正によりオプトイン規制に改められた。

一方、通信行政を管轄する総務省も、2002 年 4 月、「特定電子メールの送信の適正化等に関する法律」を制定し、広告以外のメールも含め、まず、オプトアウト規制からスタートし、2008 年、オプトイン型に改正している。スパムメールを受信した場合、総務大臣及び内閣総理大臣への申出が可能[206]で、大臣は申出を受けた時は調査をし、必要な措置を取らねばならない[207]。大臣指定の登録送信適正化機関は、申出に関する助言を行い、大臣の要請に応じ事実関係を調査する。日本データ通信協会が登録されている。大臣は、スパムメールや送信者

[206]特定電子メールの送信の適正化等に関する法律　8 条 1 項
[207] 同 8 条 4 項

情報を偽った電子メールに対し、措置命令が可能で、違反には罰則がある[208]。また、電気通信事業者は、これらのメールに対し、役務提供を拒否することができる[209]。

日本データ通信協会の迷惑メール相談センター[210]では、総務省より委託を受けて、特定電子メールの送信の適正化等に関する法律に違反していると 思われる迷惑メールを収集している。メールの転送・情報提供フォーム・又はプラグインから通報が可能である。FTC の Do not call の通報画面と同様、「提供いただいた違反情報については、総務大臣及び消費者庁長官による違反送信者への措置、電気通信事業者による送信防止対策に活用させていただきます。なお、いただいたメールの内容や送信者への措置状況などについての個別の照会には応じかねますので、あらかじめご了承のほどお願いいたします。」と記載されている。

メールは海外から送信されることも多いため、総務大臣は外国執行当局に対し、その職務の遂行に資すると認める情報の提供を行うことができる。逆に、一定の場合を除き、提供した情報を外国の刑事事件の捜査等に使用することに同意することができる[211]。

2016 年度、迷惑メール相談センターには約 1,454 万件の情報提供があり、総務省に代わって作成した警告は 3,419 件、ISP に対する送信停止等の依頼が 13,561 件（115 社）、海外の執行機関への情報提供は 42,791 件であった。[212]また、総務省は、2015 年度 10 件、2014 年 6 件の措置命令を出している[213]。

内閣総理大臣の上記権限は消費者庁長官に委任されている[214]。

6.3.2 不招請勧誘規制の趣旨と概要

通常、消費者の購買は、店舗に出向き、自由に商品や価格を比較して、自らが購入したいものを購入する。しかし、店舗を構えない事業者や、より積極的な事業者は、個別に勧誘して販売機会を得ようとする。マスに対する宣伝より、より細やかに消費者にあった情報を提供する、人間関係、信頼関係を作ってビジネスにつなげる、という面からも、これ自体は非難されることではない。しかし、その態様によっては、個人の自宅というプライバシーや安定を求める空間・時間への「侵入」でもあり、閉鎖された空間でありどのような勧誘が行われているのかわかりにくい状態でのセールストークであり、また、能動的に他の商品と比べて購入する余裕がないまま、冷静に考えると必ずしも自由な意思決定により購買を決めと言えない場合もしばしばある。

このように、消費者が招かないのに訪問、通信等を通じて商品・サービスの購入（時には販売）を勧誘する「不招請勧誘」に対する規制は、まずは、消費者保護の観点から始まった。

規制の対象は、大きくわけて以下のものがある。

①訪問

②郵送(ダイレクトメール)

---

208 同　措置命令　7 条　罰則　34 条　1 年以下の懲役または百万円以下の罰金

209 同　11 条。具体的には OP25B や送信ドメイン認証が推奨されている。

210 http://www.dekyo.or.jp/soudan/ihan/index.html

211 法　30 条　一定の場合とは、政治犯、日本では犯罪ではないもの、共助の保証がない場合。

212 http://www.dekyo.or.jp/soudan/info/index.html#katudo　(2017･9)

213 http://www.soumu.go.jp/main_sosiki/joho_tsusin/d_syohi/m_mail.html　(2017.9)

214 法　31 条

③電話（FAX、固定電話、携帯電話）

④電子メール

広告規制や態様の規制だけでなく、勧誘自体を禁止するのが不招請勧誘規制である。

前述のとおり、日本では、電話について、消費者が契約を拒否した場合の架電禁止[215]と電子メール[216]のオプトイン規制が不招請勧誘規制にあたる。

世界では、特に③の電話勧誘についてはすでに 18 か国で導入されており、Do not call 制度と呼ばれている。電話勧誘は、個人の家庭という平穏なプライバシー空間・時間を突然乱すものであり、不意打ち性、匿名性、密室性、即断の強要、不確実性、勧誘の執拗性、事業者側の勧誘の簡便性・安価性、という特質から、迷惑であり、消費者の適正な自己決定を損ないやすいからである[217]。

また、①の訪問販売についても、拒否する意思表示を行った消費者への訪問販売を禁止する Do not knock 制度がある国・都市もある[218]。

6.3.3 世界の Do not call 制度[219]

世界では既に 18 カ国で Do not call 制度が導入されている。（表 **20** 参照）消費者に負担をかけずに勧誘を拒絶でき、優れた制度と思われる。

表 20 各国の Do not call　制度

	国	運用開始年	根拠法	規制当局	オプトIN/OUT	勧誘拒絶リスト取得？リスト洗浄？	テレマーケッタの運用費用負担
米州	アメリカ	2003	FCC:通信消費者保護法 FTC：テレマーケティングと消費者詐欺および不正行為防止法、テレマーケティング販売ルール 州法	FCC(連邦通信委員会) FTC(連邦取引委員会) 州検察 <運営は FTC>	ＯＵＴ	勧誘拒絶リスト取得	有料
	カナダ	2008	2005 年改正電気通信法	ラジオテレビ通信委員会 <運営はベルカナダに委託>	ＯＵＴ	勧誘拒絶リスト取得	
	メキシコ	2007	連邦消費者保護法	連邦消費者検察局(PROFECO)	OUT	勧誘拒絶リスト取得	有料
	ブラジル（いくつかの州）		全国レベルは法案段階 州や市 通信事業者は国家電気通信庁の規則	州や市の消費生活センター 違反にはブラジル消	OUT	勧誘拒絶リスト取得	有料

215 特定商取引法 17 条

216 特定電子メールの送信の適正化等に関する法律第 3 条、特定商取引法 12 条の 3

217 齋藤雅弘、他、『特定商取引法ハンドブック（第 5 版）』215 頁（日本評論社、2014）

218 オーストラリア、米国では市レベルの自治体（オハイオ州パーマ市など）が実施。大濵巌生=カライスコス・アントニオス「世界の勧誘規制を知る　第 12 回　オーストラリア・アメリカの Do-Not-Knock 制度」『国民生活』2016 年 5 月号 17 頁

219 薬袋 真司ほか「世界の勧誘規制を知る」　『国民生活』2015 年 6 月号～2016 年 7 月号(2015～2016)
http://www.kokusen.go.jp/wko/data/bn-kkisei.html　(2017.2)
内閣府消費者委員会第 6 回特定商取引法専門調査会（2015 年 6 月 10 日）資料 1　35 頁～40 頁

				費者保護法典 56 条の罰則、業務停止			
	アルゼンチン	2015 全国	創設：2014 年法律第 26.951 号 事業者の義務： 個人情報保護法	司法省所轄の、個人情報保護局（PDP)	OUT	勧誘拒絶リスト取得	有料
欧州	欧州指令	2009	電気通信分野における個人データ処理及びプライバシー保護に関する指令（2009/136/EC)		IN or OUT		
	イギリス	1999	個人情報保護法 電気通信プライバシー法	規制：通信局（Ofcom) ＜ダイレクトマーケティング協会に運営委託＞ 執行：情報委員局（ICO)	ＯＵＴ	勧誘拒絶リスト取得	有料
	フランス	2016	消費法典 2014 年ハモン法による改正）	経済財政産業省の競争・消費・不正防止総局 ＜運営はテレマーケティング 4 社による簡易株式会社＞	OUT	リスト洗浄方式	有料
	イタリア	2011	2010 年大統領令第 178 号 違反者は、個人データ保護法典により制裁	経済開発省 ＜運営は公益活動財団＞	(非登録者は、の黙示の意扱い問い)	リスト洗浄方式	有料
	ノルウェー	2001	市場統制法	いくつかの公的レジストリを管理する政府機関	OUT		
	デンマーク		消費者契約法	中央個人登録局	IN	勧誘拒絶リスト取得	無償
	ベルギー	2013	電気通信法	経済省 ＜運営はﾍﾞﾙｷﾞｰﾀﾞｲﾚｸﾄﾏｰｹﾃｨﾝｸﾞ協会が設立した非営利団体>	IN	参照	
	オランダ	2009	電気通信法	消費者・市場当局 ＜運営は財団＞	ＯＵＴ		
	スペイン	2009	個人情報保護に関する組織法 電気通信一般法 情報社会及び電子取引サービス法	個人情報保護局 ＜運営はスペイン・デジタル経済協会＞	ＯＵＴ？2014 年勧誘事前同意必要）	勧誘拒絶リスト取得	基本有料
	アイルランド			通信規制委員会 情報保護委員会	ＯＵＴ		
アジア大洋州	オーストラリア	2007	Do Not Call Register Act 2006	オーストラリア通信メディア庁	ＯＵＴ	リスト洗浄方式	基本有料
	シンガポール	2014	個人情報保護法	個人情報保護委員会（PDPC)	OUT	リスト洗浄方式	有料
	韓国	2014	訪問販売法	公正取引委員会 ＜運営は消費者院＞	OUT	リスト洗浄方式	勧誘事業出料負電話販売は届無が制。(国担)
	インド	2010	電気商用通信加入者プレファレンス規則	インド電気通信規制委員会（TRAI)	OUT	勧誘拒絶リスト取得	テレマーケッターは登録義務。

この制度は、1999 年英国でダイレクトマーケティング協会の自主規制として始まった。米

国では2003年に導入した。多くの国では、米国と同様、勧誘を受けたくない者が登録する「オプトアウト方式」を取っている。

2009年EUは「電気通信分野における個人データ処理及びプライバシー保護に関する指令（2009/136/EC）」において、各国にDo not call制度の導入を義務づけた。そこでは、ダイレクトマーケティングを目的とする自動電話、ＦＡＸ，電子メールはオプトイン、それ以外の通信（電話を含む）は、オプトインでもオプトアウトでも可、とした。これを受けて、ベルギーやデンマークでは、勧誘を受けてもよい者が登録する（つまり、デフォルトは勧誘禁止）オプトイン方式を取っている。

根拠法は、消費者保護系、通信行政法系が多いが、シンガポールやスペインなど、個人情報保護法によるものも出てきている。規制当局も、同様に消費者保護系、通信行政系、個人情報保護系があるが、規制は通信行政系、違反への執行は個人情報保護系、という国もいくつかある。アメリカの場合は、FTC自身がDo Not Callシステムの運営をしているが、規制当局が運営を外部に委託する国も多い。委託先は、通信会社やNPOもあるが、ダイレクトマーケティング事業者の事業団体に委託している国も複数ある。これは、法制度化される前に、電話勧誘への批判の高まりから自主規制を行っていた歴史による。

消費者は電話番号のみ登録すればよい国と、事業者には電話番号しかアクセスさせないが、成りすまし防止で身分証明番号まで登録させる国もある。事業者は、月に一度、登録リストと自らの電話勧誘用リストの照合義務がある。直接照合義務を課す国と1か月以上前に登録された電話番号への勧誘に罰則をつけることで間接的に義務を負わせている国がある。リストのアップデートには、事業者に登録リストをダウンロードさせて自らの電話勧誘用の架電リストと照合させる「勧誘拒絶リスト取得方式」が多いが、最近は、余計な情報を渡さず、架電リストを提出させ運営主体側で削除して返却するリスト洗浄方式の国も増えている（豪、星、韓、伊）。また、多くの国で、テレマーケティングを行う事業者に登録義務を課し、リストの利用に料金を徴収してDo not callシステムの運営費用を賄っている。

すべての国で、米国と同様、勧誘の同意を得ている場合や既存取引のある場合は登録された電話番号に対しても、勧誘可、として、利用と保護のバランスを取っている。政党や一般紙が適用除外となっている国も複数ある。

登録したのに勧誘があった場合に公的機関などに苦情申立可能な国も多く、Webなどで簡単に通報できる仕組みを提供している国もある。すべての国で、リストされている電話番号への勧誘電話など違反には罰金を定めており、かなり高額[220]である。中には、インドのように、違反事業者には通信切断し、2年間ブラックリストに掲載する国もある。

ほとんどの国が海外からの電話勧誘にも適用ありとしているが、実際の強制に悩んでいる[221]。しかし、Do not callやスパムメールなどの不招請勧誘規制に関する国際協力の動きもある。複数の関係機関で構成するUnsolicited Communications Enforcement Network (UCENet)[222]を活用し、協力して対応している。例えば、2015年には、カナダのラジオテレビ通院委員会と米国のFTCが協力してカナダのDo not call違反について米国の事業者に罰金を科すことに成功

[220] 例えば米国では最高16000ドル
[221] 内閣府消費者委員会・前掲注219
[222] https://www.ucenet.org/

している[223]。日本からは、外務省と消費者庁がメンバーとなっている。特定電子メールの送信の適正化等に関する法律上の、通信事業者以外への権限行使が消費者庁に委任されているからであろう。

6.3.4 個人情報保護法秩序における不招請勧誘規制の新たな役割

各国に見るように、1990 年代のテレマーケティングの発達と横行を踏まえ、電話勧誘が社会問題化した国々では、欧州では通信販売業者の自主規制としての Do not call 制度が試みられ、FCC による通信規制法としての規制、FTC による消費者保護法としての規制が導入されてきた。

1995 年 EU 個人情報保護指令を受けて 2000 年頃までに欧州各国が個人情報保護法ができるまでに、これらの体系で一定の規制ができていたが、目的外利用を禁止する個人情報保護法と重複する部分が多く、関係整理が必要となった。EU では、通信規制法の域内標準化を狙った 2002 年 e プライバシー指令で、1995 年指令を踏まえた通信プライバシー規制という位置づけで、不招請勧誘規制が定められ、前述のとおり、電話はオプトイン又はオプトアウト、FAX と SMS はオプトインとした不招請勧誘規制を整備することが求められた。表 **20** にあるように、各国は、電気通信法や消費者関連法で規制している。一方、スペインやシンガポールのように、個人情報保護法で規制する国もある。シンガポールでは、2012 年個人情報保護法 36 条から 48 条で Do not call を定め、個人情報保護法を担当する personal data protection commission(PDPC)が Do not call も運営している。

このように、不招請勧誘規制と個人情報保護の二つの制度は互いに密接な関係にある。英国では、Do not call 制度の運営は通信局がダイレクトマーケティング協会に委託して行っているが、執行は個人情報保護を担当する情報委員局（ICO）が担当している。6.2.2 節で述べたように、FTC は、個人情報保護も Do not call も同じ不公正・欺瞞的行為として執行しており、執行等のレポートにおいても”Privacy & Data Security”として同じジャンルで取り扱っている[224]。同じ Consumer Sentinel データベースから苦情を取り上げており、優先的に調査すべき対象の選択に DNC の苦情が多いことも端緒のひとつと考えられる。

更に、不招請勧誘規制の検知力を個人情報保護法違反発見の端緒とした事例が、2017 年 1 月、イギリスで公表[225]されている。

GSM アソシエーションは、消費者から携帯向けのスパムメールの苦情を受付け、不招請勧誘の苦情を集約し各国の法執行機関がアクセスできる「7726(SPAM)システム」に送る Spam Reporting Service を提供している。英国の個人情報保護を主管する ICO は、Spam Reporting Service の苦情データベースから、2015 年 6 月 19 日から 9 月 21 日までに、174 の pay day loan についての勧誘メールの苦情があることを発見した。調査の結果、発信元が The Data Supply Company（DSC）というデータブローカーであることを確認し、DSC が 580302 件のデータを

---

[223] *Cross-Border Investigation Between CRTC and FTC Results in Monetary Penalties for Violators,*, April 28, 2015 https://www.ucenet.org/news/cross-border-investigation-between-crtc-and-ftc-results-in-monetary-penalties-for-violators-3/

[224] https://www.ftc.gov/reports/privacy-data-security-update-2016

[225] Information Commissioner’s Office, in re The Data Supply Company Ltd, 2017 年 1 月 27 日 https://ico.org.uk/media/action-weve-taken/mpns/1625862/mpn-data-supply-company-20170130.pdf (2017.5)

購入し、21045 件のテキストメッセージを送ったことが判明した。DSC は、複数の金融機関から取得し、それらは Web サイトに同意文言を掲載している、と主張したが、ICO は、マーケティング目的でのテキスト、電子メール、自動電話に使うためにリストを売買するためには、一般的な同意文言ではなく、Electronic Communications Regulation 2003 により、具体的な送信人に対して同意が必要とした。更に、これらの目的にリストを売るには、data controller はいつ、どのようにして誰から、どう説明されて同意を得たのか、の、記録が必要とした。上記の理由により､英国の個人情報保護法である Data Protection Act 1998 の 55A 条に基づき、2 万ポンドの罰金を科した。

このように、不招請勧誘の苦情の分析により、個人情報の流通を検知することができる。

6.4 提案

5 章で述べたように、個人情報の流通を検知するためには、不正利用のモニタリングが有益であり、これが大量に漏えいするが気付きにくい故意の不正アクセスや内部犯行による漏えいを検知する力の差をもたらしているとも考えられる。不招請勧誘規制は、経済的損害やなりすましの被害につながる情報ではないが消費者へのコンタクトにつながる情報が不正に利用されていることを検知し、それが流通していることを調査する端緒となり始めている。不招請勧誘規制には、単に電話をかけない、という消費者保護だけでなく、個人情報の漏えいを検知し、breach notice により個人に自衛を可能にし、政府の積極的な執行により本当に個人情報保護法を実効性のあるものにする、という新な役割が期待できるのではないか。

しかも、消費者は登録するだけで、運営主体にリストを提出するテレマーケタの少なくとも架電リストから個人情報を削除してもらえる。運営主体にリストを提出しない事業者は、違法として取締られる。更に、苦情も FTC や GSM アソシエーションのように簡単に登録できれば、悪質な事業者には、その後の交渉や提訴を要することなく、個人情報保護委員会による執行を通じて、架電リスト以外からも削除させることができる。

これにより、消費者と真面目な事業者に過剰な負担を負わせず、保護と活用のバランスが取れ、悪質な事業者に対する発見と積極的な調査により、不正な流通を取り締ることができる実効性のある制度や運用に向けた大きな一歩となるのではないか。

7　日本における「不適正」流通への執行強化とバランスのとれた法規範に向けて

7.1 概要

2 章で述べたように、日本においては、個人情報保護法の執行はアンバランスであり、不適正流通や不適正利用への執行は、2015 年改正を受けて緒に就いたばかりである。これまでのアンバランスな執行の結果、消費者の不安は解消されず、適正に取得した事業者の安全管理にのみ制度が支えられ、一旦、事故が起こると、社会的批判や損害賠償請求がそのような事業者に向けられる。流通を検知する仕組みもサービスもなく、侵害通知への対応も、二極化している。

不適切な利用を行う下流の事業者の半分くらいは、本当はレピュテーションも気にするはずのまともな事業者もいる[226]。2015 年個情法改正により、実体法的にも違法のケースが増えるので、報道等でもそのように扱うことにより、表 1 の８のレピュテーションによる事実上の強制で効率的に牽制できるかもしれない。中流の名簿販売事業者についても、一部の事業者は「日本個人データ保護協会」なる NPO を作っているようなので、認定個人情報保護団体にすることで、合法的に流通する事業者も出てくるかもしれない。

しかし、レピュテーションを気にしない事業者や名簿販売事業者については、表 1 の 1. の法執行しかない。ここが低調だったことが問題の一因であったことは、前述のとおりである。

個人情報の不適正利用の検知力を上げなければ、執行に向けた調査もできない。1.3 節図 **3** の中流、下流における「不適正」な流通に対し、もっと執行が行われ、自分が知らないところで自分の情報が取引され使われている、という消費者の不安を取り除けるようにしなければならない。そうでなければ、漏えいしてしまった図 3 の上流の②の事業者を責めて終わりになり、流れた情報は放置されたままである。

このアンバランスな状況を変え、消費者の不安を減少させるには、表 18 に示した課題に対応して表 21 に示すように、以下の対応が必要である；

①バランスのとれた侵害通知

②2015 年改正法による不適正流通や不適正利用事業者への執行強化

③2.5 節で述べた、2015 年改正法による不適正な流通への運用強化のための残課題の解消

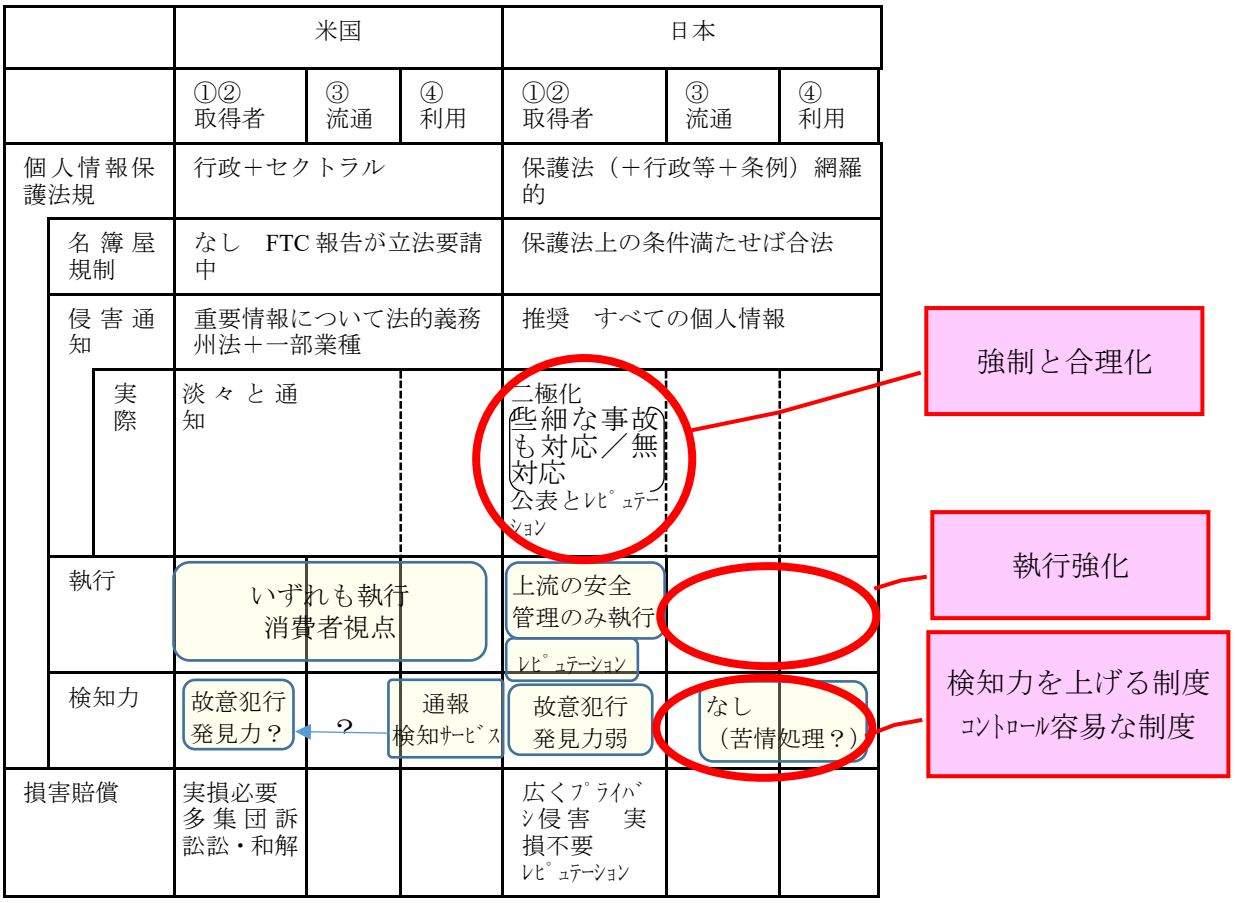
③－１　委員会 web 上の事業者も含め、名簿販売事業者に対する容易な開示請求

③－２　流通・利用の検知力強化

以下、順に詳説する。

[226] 2014 年の大量漏えい事故の際は、一時期日本語ワープロを支えたパソコンソフト事業者や、著名な英語教室も購入していた。

表 21　日本の状況の要改善ポイント



7.2 侵害通知

アンバランスな一つの政策は、侵害通知である。

真面目な事業者だけが神経質に実施し、レピュテーションを気にしない事業者は全く何もしない、という状況は、消費者を守る観点からも改善すべきである。現在の日本で推奨とされる侵害通知を合理化した上で義務化し、隠れていたインシデントを見える化できるようにすべきである。

法的に義務を課すのは、米国のように、経済的被害や詐欺被害などが予想される情報に限るべきである。こうすることで、取引コストとメリットをバランスさせた制度とすることができる。もちろん、他の情報でも個人に警戒、自衛してもらう必要はあるので、本人通知は現状の通り、推奨とするが、官庁報告は不要だろう。公表は、米国・欧州と同様、本人に連絡をつけることができない場合の代替手段とすべきである。必要な人には伝わっているので、「世の中に詫びないのはおかしい」、「隠蔽である」、という論調で SNS などで批判すべきではないだろう。そのように社会にも政府から啓発すべきである。お客様第一で細かな配慮をすることを否定はしないが、お客様からのレピュテーションはともかく、その基準で社会的

に制裁論調になるのは卒業したい。もちろん、事の重大性と規模から、公の関心事として公表すべき事態は、個人情報保護法の義務、推奨の世界を離れて、広報的判断から公表されるべきであり、そこでは個人情報保護法の侵害通知に関する規定や規則は無関係であるべきである。

法で義務付けた範囲を超えた、例えば基本 4 情報や連絡先などの漏えい時に本人に通知する事業者にはなんらかのインセンティブがあるようにすべきである。例えば、今でも論理的には不可能ではないが、個人からの損害賠償請求において、通知することで自衛を可能にしたことが損害額減少の理由となることを、何らかの形で普及させることが考えられる。義務でもないのに本人にお知らせする事業者を評価する論調も、期待したいところである。

政府への報告の目的も再整理すべきである。報告してきた事業者に安全管理義務違反で執行することより、米国のように、流れてしまった情報の不正利用の捜査や不正アクセスなどの犯罪行為の捜査に結びつけることを目的とすべきである。これは、そもそもの個人情報保護の目的である個人の保護や消費者の保護・安心につながる政策であり、次節以下で述べる中流、下流への執行とも整合する。

7.3 2015 年改正法の運用強化と検知力アップ

2.5 節で詳説したとおり、2015 年法改正では、名簿販売事業者をターゲットとした規定が実体法上入れられた。トレーサビリティについては、多くの真面目な事業者には負担がかかるが、不適正な流通の取り締まりのためには、有益だろう。それだけに、実際に利用や流通を検知し、執行してもらわなければ、ますます真面目な事業者と不適正な中流の名簿販売事業者、下流の不適正な利用事業者とのアンバランスが大きくなる。

前述したとおり、名簿販売事業者への執行が低調だったのは、主務大臣制の下、担当官庁がなかったことが一つの原因であるが、改正法が施行された現在においては、個人情報保護委員会が一元的にすべての事業者を対象とするため、その積極的な調査と権限行使が期待される。個人情報保護委員会には立入検査権もできたので、検知されれば内偵のうえ、動けるはずである。

個人情報保護委員会では、相談ダイヤルを設置し、直接苦情を受け付けている[227]。同サイトでは、できること、として、以下を上げている；

1 個人情報保護法に関する一般的な質問への回答
2．苦情の内容を所掌する他の相談窓口の紹介
3．苦情の相手方事業者への苦情の内容の伝達（委員会が必要と認めた場合）
4．個人情報保護法に定められた義務に反する行為があった場合の監督部門への取次ぎ
5．苦情をめぐって、苦情の相手方と争いが生じた場合のあっせん

現状の消費者センターの斡旋窓口のような消極的な表示に見えるが、真面目な事業者の心配を考えるとこのような表示になるのだろう。認定個人情報保護団体に属している企業は、基本的に遵法精神は高いと思われるため、そこに内容を伝達し、もし、消費者が誤解しているようなら誤解を解き、敵対的でない解決方法を探れるようにするためのものと思われる。

[227] http://www.ppc.go.jp/application/pipldial/

不適正な流通への検知力を上げるためには、従来からの消費者センターへの苦情受付について、個人情報の不正利用や不正流通を取り上げやすい形で PIO－NET で共有し、米国の FTC の Consumer Sentinel のように、件数や規模、影響、内容の観点で、悪質なものから優先的に積極的に取り上げ、内偵して捜査すべきである。また、効率的に分析するためにも、FTC の通報サイトなどの確認項目が参考になるかもしれない。また、FTC のように、Web での苦情受付も有効だろう。FTC のように、1 件 1 件に対応するとは限らず、全体として重要なものを検知するためのものであることを明示すれば、自分の苦情がすぐに取り上げられなくても消費者も理解するだろう。もちろん、集まった苦情の検討分析の過程で、為にする通報などを除外する手法も必要である。

改正後の現行法では、個人情報の利用事業者から遡ることが可能になる。提供した覚えがない事業者からコンタクトがあった、という、「不正」利用の相談を端緒として、当該利用事業者に任意や 40 条に基づく報告聴取や資料提出請求で情報収集する。利用事業者については、実体法上、適正な取得、利用目的公表、取得の記録が使えるが、記録から取得の「適正」性を調査できる。また、記録から入手先に対し、同様に任意や 40 条に基づく情報収集をし、当該事業者が、オプトアウトによる第三者提供の届け出をしていなければ、その時点で、41 条に基づく指導か、42 条に基づく改善勧告が可能になる。場合によっては立入検査権を発動することもできる。

法改正までに入手されてしまった情報には記録作成義務はかからないが、不適正な流通に対しては、従来に比べるとかなり大きな成果にはなると考える。主務大臣制とは違い、すべての業種の事業者の調査権限をもった個人情報保護委員会には、不訂正利用の積極的な調査を期待したい。万一、調査がされない場合、2015 年の改正行政手続法 36 条の 3 により、処分等の求めをすることができる[228]。申出を受けた行政庁は調査義務があることから、これを活用することも効果的かもしれない。

次節以降では、もう少し、創造的な制度も提案したい。

まず、本人関与原則に基づく権利行使を、より本人の負担を減らして行う方法である。その際、将来的に各国のように、Do not call が導入されることを予想しつつ体制を考える。次に、期が熟せば導入されると思われる Do not call を検討する。その際、不適正な流通により保有される事業者を見つけ出し、削除させる Do not hold に発展させることも検討する。

7.4 個人情報保護法上の利用停止・消去請求の代理人としての外郭団体

個人情報保護委員会の強制力は、苦情の多い悪質なケースを優先的に行使することになる。個々のケースに対応することを保証するものではないため、不審なコンタクトを受けた消費者の個々のケースへの対応は、依然、苦情処理プロセスや本人関与原則に基づく権利を使いながら、当事者が対応することになる。

事業者に対し本人関与の原則に基づく個情法 28 条から 30 条の権利を行使し、保有している自分の情報の開示を求め、また、利用停止を請求するにも、信用できるかどうかわからな

[228] 蔦大輔「監督官庁による適切な法執行を促すために」NBL1103、74 頁

い勧誘者やその上流の名簿販売事業者に対しては、不安がある。請求された事業者は、本人確認方法を定めることができる[229]。本人ではない者の請求により、事業者が誤って（騙されて？）情報を開示し、消去することにより生じる本人への不利益や無用な紛争を防ぐために本人確認が必要であることは十分理解できる。しかし、相手が信用不明の事業者の場合、更に自分の個人情報を提供することになり、個人としては大いに躊躇するところであり、実効性が期待できない場合がままある。

このハードルを下げる方法として、本人が権利行使を委託できる団体をつくり、その団体からの請求については、本人についての追加的な本人確認書類を要求しないで開示、訂正、利用停止、削除に応じても事業者には過失はない、という権限を与える。これは、政令 10 条 1 項 3 号の運用に関する事項なので、政令か規則で可能になるのではないか。但し、この動きが非弁活動と言われないためには法的措置が必要かもしれない。

この団体は、消費者が安心して個人情報を登録できるよう、信用のある者に限る必要がある。認定個人情報保護団体にその役割を担わせることも考えられるが、法 47 条 1 項によれば、その権限は、業務の対象となる個人情報取扱事業者等の個人情報等の取扱いに関する苦情の処理等であるため、消費者は、事業者が認定個人情報保護団体に属しているのか、どの認定個人情報保護団体なのか、を探さなければならず、効率的ではない。一元的に 1 つの外郭団体を作るべきである。

前述のとおり、この制度は、将来的に Do not call が導入されるときには、それを個人情報の流通や不正利用の検知に利用する制度に発展させる。従って、将来的に Do not call が導入されるときは、この団体を運営主体と（以下「運営主体」という）とすることを想定する。利用停止・消去の代理人であるこの団体には、必然的に自分の情報をコントロールする意思のある消費者の個人情報が集まるので、効率的でもある。米国では、Do-not-call の運営は FTC が自ら行い、電話マーケティングを望まない消費者は FTC に登録する。日本においては、個人情報保護法の実効性につなげる、という目的から考えると、個人情報保護委員会が主管し、消費者庁が共管する外郭団体を作るのが望ましいと考える。消費者庁を共管とするのは、個人情報保護法の苦情処理を地方公共団体やその消費生活センターが担っていること、Do not call となった時には、消費者保護の役割の方が大きいからである。

政府機関でなく外郭団体とするのは、この段階では私人の代理人の役割なので、政府機関が担当するのに馴染まないからである。また、住民基本台帳訴訟なども考え合わせると、政府そのものによるよりも、外郭団体が運営し政府は登録データにアクセスしないのが望ましい。

まず、本人は「運営主体」に登録する。この際、本人確認に必要な証明書を「運営主体」に提出する。立法的措置（政令以下レベルかもしれないが）は必要かもしれないが、「運営主体」からの請求については、事業者は本人確認があったとみなし、本人確認書類を要することなく請求に応じることとする。こうすることによって、事業者に更なる個人情報を提供することなく、本人関与原則上の権利を行使することができる[230]。この請求を受けても消去し

---

[229] 個情法 32 条 1 項、施行令 10 条 1 項 3 号

[230] 同様に、ある法的地位を証明するために、プライバシー上、提供したくない情報を提供せざるを得ない状況を立法的に解決した例として、「法定相続情報証明制度」がある。
家族が亡くなり、銀行等々の相続手続きを行うとき、金融機関等は、後日、相続人が出てきてトラブルになるの

ない事業者に対しては、個人情報保護法に定めた行政による処分のプロセスが動くことになる。

利用とのバランスについても、そもそも、個人情報保護法上、消去を求めることができるのは、利用目的を超えた利用と不正手段による取得だけであり、利用を新たに抑制するものではない。通知または公表を行った利用目的内で利用していれば、「運営主体」を通じてそれを説明すれば、よいだけである。また、プライバシーマークでは、それ以外の場合も、本人の求めに応じて消去することになる[231]が、その場合でも、事業者が利用停止・消去請求を受けた際、過去、直接同意を得て収集されているのであれば、その旨の説明や、利用停止・消去の場合の不利益の説明などを「運営主体」を介して本人とコミュニケーションし、それでも本人が消去を望むなら消去するという保護と利用のバランスを取ったプロセスを踏むことは、本人が直接請求する場合と同様である。

登録時に「運営主体」に本人確認のための証明書を提出しているので、個々の権利行使依頼にあたっての本人確認は、オンラインでの認証も可能とすべきである。

事業者にとっては、消去請求されている情報が自らのリストのものと類似しているが、更なる情報がないと同一人物の情報か判断できない場合もある。その場合、「運営主体」から更に情報を提供させるのではなく、事業者から類似のものを提供して「運営主体」で確認するプロセスにすれば、余計な情報を更に提供する、という心配もなくなる。

7.5 Do-not-call

7.5.1 Do not call の具体的提案

迷惑な不招請勧誘といえば電話と訪問である。訪問勧誘では、勧誘事業者は必ずしも訪問先の個人情報を持つ必要はなく、並んでいる住宅を順に訪問する場合が多いだろう。電話でも、自動電話によればそれは可能だろうが、今のところ、日本ではそれほど普及せず、同窓会名簿から流れた情報など、何らかの名簿に基づくことが多い。従って、下流の不正利用検知には、Do not call 制度を活用することができると考える。

英国の ICO の例のように、電子メールによる不招請勧誘の情報を活用して、漏えいを検知

を避けるため、被相続人の生まれてから死ぬまでの戸籍謄本を要求する。もし故人が独身なら、その両親の生まれてから死ぬまでの戸籍謄本も必要となる。これらは、普通の人の感覚ではあまり開示したくない機微な情報を含む。これを金融機関、通信サービス会社、会員制のサービス等々、故人の取引先から求められる。金融機関には消費者金融などもあり、また、会員制サービスなども、必ずしも信用できるかどうかわからないものもあり、提出した戸籍謄本が本当に機密管理されるのか、情報が流されないのか、不安に思うこともある。
2016 年 12 月 22 日、法務省は、相続手続きを簡素化する「法定相続情報証明制度」新設のために、「不動産登記規則の一部を改正する省令」の改正を提案し成立。2017 年 5 月 29 日よりスタートした。
http://www.moj.go.jp/MINJI/minji05_00284.html
その目的は、大量の相続関連書類を集めて複数事業者に提出する負担を軽減するため、とされているが、プライバシーの保護、という意味でも有意義と考える。この制度では、相続人が、法定相続情報一覧図を作成、関係戸籍謄本と共に登記所に提出すると、登記所が認証文を付記した証明書を発行するもので、金融機関などでは証明書の写しの提出だけで手続きが行える。証明書には、被相続人は住所記載するが、相続人は、氏名、生年月日、続柄のみでよく、住所の記載は任意とされている。
この制度では、登記所が、ここで提案している団体と同様、プライバシー上、出したくない情報を相手方に渡すことなく、法定の権限により一定の事項を証明する役割を果たす。

[231] JIS Q 15001:2006　3.4.4.7

することももちろん可能である。6.3.1 節で述べたように、既に、日本には電子メールによる不招請勧誘のクレームを届け出る仕組みもあり、個人情報保護委員会は、ここをモニターすることは、今でも可能であろう。しかし、プライバシー空間侵入への不安を与えるという点では、住所と電話番号であろう。本来は、住所情報を持っていることの検知ができればよいのだが、実際に Do not call のようなマッチングを行うとなると、数字だけを扱う電話番号に比べ、よりシステムとその運用が難しいと考えられ、まずは、多くの国で運用されている Do not call から始めるべきとかんがえる。

勿論、不招請勧誘による消費者の迷惑や詐欺被害、不安の解消が主目的であり、個人情報の不正利用検知はそれを利用するものである。すでに先進国を中心として 18 か国に導入されており、将来的に日本において導入してもおかしくない。

電話勧誘対策としては、まず、その前に、特商法の行政機関の調査権限に電話をかけてくる相手を特定する権限を持たせる必要がある。特商法第 66 条第 4 項では、行政は電気通信事業者に対し、使用者を特定するために必要な情報の報告を求めることができるが、対象は電子メールや Web サイトだけのようで、電話番号は対象になっていない。従って、名称がはっきりしない事業者を電話番号から割り出すことが可能なのは捜索差押許可状で請求できる捜査機関だけであり、間接罰しかない特商法では難しい。これは、現在の電話勧誘規制の執行のためにも必要であり、Do not call の導入の前提としても違反者を取り締るために必要である。

次に、Do not call の導入について、必要性を徹底して議論する必要がある。

2015 年の特商法改正の際、消費者代表や消費者庁が、電話勧誘と訪問勧誘についてオプトイン方式の不招請勧誘規制を導入しようとして、新聞協会などから猛反対を受けて法案に入れることを断念した経緯もある[232]。また、欧州では、1990 年代から、テレマーケティングへ

---

[232]日本ネット経済新聞「内閣府・特商法専門調査会/電話勧誘めぐり紛糾/過剰規制に通販業界が猛反発」、2015 年 07 月 30 日　http://www.bci.co.jp/netkeizai/article/921　(2017･6)
内閣府消費者委員会第 6 回特定商取引法専門調査会（2015 年 6 月 10 日）では、各ヒアリング対象者から提出された資料として、以下が配布されている；
＜一般社団法人日本新聞協会＞
資料２-１-１「特商法見直しに関する日本新聞協会の意見骨子」
資料２-１-２「特定商取引に関する法律見直しに関する日本新聞協会の意見」
資料２-１-３「新聞販売の現状」
資料２-１-４「新聞販売綱領」
資料２-１-５「新聞購読契約に関するガイドライン」
＜公益社団法人日本新聞販売協会＞
資料２-２　「特定商取引法見直しに関する意見」
＜一般社団法人太陽光発電協会＞
資料２-３-１「訪問販売・電話勧誘販売等の課題についての意見書」
資料２-３-２「失敗しない太陽光発電システム選び」
資料２-３-３「太陽光発電協会　販売基準」
資料２-３-４「太陽光発電協会　表示ガイドライン（平成 26 年度）」
＜株式会社ダスキン＞
資料２-４　「ダスキンの訪問販売事業について」
＜一般社団法人自動車販売連合会＞
資料２-５　「特定商取引法の見直しについて」
＜株式会社髙島屋＞

の批判が高まり、業界団体が自主的に Do not call を運用していたため、義務化された時の抵抗はそれほど大きくなかったと思われる。また、南米やオーストラリアのように、州や市で義務化し始めた後に国の法律で義務化した国も、それほどのサプライズではなかったと思われる。しかし、そもそも海外でこれほど Do not call 制度が普及していることを知らされていない日本では、事業者を中心としてかなり抵抗があると思われる。特に、事業者のリスト照合の負担と、それほど高額ではないもののリスト利用料の経済的負担などを考えると、かなりの反対が予想される。

議論の結果、導入することとなった場合に、個人情報の不正利用検知も睨み、また、事業者負担を減らした制度としては、どのようなものが考えられるだろうか。

まず、いくつかの国のように、政治、新聞など、国民の知る権利や言論の自由にかかるものは適用除外にすることで、新聞協会の理解を得る。そして国民の理解とテレマーケティング事業者の理解を醸成して Do not call を実現する。

英国では、通信事業者への動機づけとして、電話勧誘を希望しない個人へ電話をした場合、契約成立に至る可能性も低いことから、コストパフォーマンスが低く、更にスタッフの士気が下がり販売に否定的な影響を与えるため、Do not call 制度は事業的なメリットがあること、更にオプトイン規制導入の圧力を抑制できることがあげられている。事業者への説得に参考となると思われる[233]。

いくつかの国の制度のように、制度や規制と執行機関が不整合でもおかしくない。Do not call 制度自体は消費者保護の側面が強いので特定商取引法上の制度とし、リスト参照義務、架電禁止、コールリスト上の削除義務までを消費者庁の執行とするが、個人情報保護委員会も連携し、Do not call 違反やその苦情を端緒として不適正な入手・流通・利用への立入検査権の行使も可能とする。

既に個人情報保護法で事業者が萎縮しているわが国では、個人情報の利用と保護のバランスの観点からは、多くの国と同様、架電を望まない人が登録する「オプトアウト方式」を取るべきである。なりすまして他人の電話番号を登録することの防止のために、氏名、住所などを登録することは必要としても、多くの国と同様、事業者リストとの突合は電話番号だけにするのが、プライバシー上も技術上も負担が少ないだろう。多くの国と同様、テレマーケティングを行う事業者に有料で登録を義務付け運営費用を賄うのが望ましい。更に、名簿事業者についても登録を義務化して、事業者規制的なアプローチを可能にする。

プライバシー上だけでなく、7.4 節で提案した代理人としてのアクションを取るためにも、また、個人情報保護法の執行ツールとしても、シンガポールや韓国のようにリスト洗浄方式

資料２-６　「電話勧誘販売の状況について（アウトバンド事業について）」
第 9 回特定商取引法専門調査会（2015 年 7 月 31 日）の中間取りまとめ(案)骨子には、「第 4 回、第 6 回、第 8 回の議論を踏まえ記述」とあるが、最終回である第 18 回に出された特定商取引法専門調査会報告書（案）によれば、「審議の過程において実施された関係団体からのヒアリングの結果、勧誘に関する規制強化に対し反対する意見が示された。また、中間整理に関する集中的な意見受付に寄せられた意見のうち、勧誘に関する規制の論点に係る意見は、賛成 545 件、反対 39,428 件であった」と、反対意見にかなりの動員が推測された様子がうかがえる。
http://www.cao.go.jp/consumer/history/03/kabusoshiki/tokusho/senmon/006/shiryou/index.html
http://www.cao.go.jp/consumer/history/03/kabusoshiki/tokusho/doc/20150731_shiryou3.pdf、
http://www.cao.go.jp/consumer/iinkaikouhyou/2015/doc/20151224_tokusho_houkoku2.pdf

[233] 薬袋・前掲注 219　2015 年 7 月号 17 頁

の方が望ましい。なぜなら、事業者から何らかのコンタクトがなければ消費者はどの事業者が自分の個人情報を持っているかわからないのが普通であり、勧誘事業者に架電リストを提出させるリスト洗浄方式であれば、消費者に負担をかけることなく運営主体を通じて自分の情報を持っている事業者を発見することができるからである。

運用にあたっては、事業者の負担を減らす工夫をすることが求められる。そのためには、輸出管理におけるモデルコンプライアンスプログラムのように、内部管理を整備させ、政府又は運営主体が監査・認証した事業者には負担が軽くなる仕組みがあった方がよい。整備させる内部管理の内容は、制度の趣旨から考えて、①基本的に間接取得をしない、②間接取得（第三者提供を受ける）場合は「運営主体」に報告する、③改正個人情報保護法に基づく第三者提供授受時の記録義務を果たしている、④直接取得についても、個々の個人についていつどのような利用目的に同意したのかが管理されている、ということが要請されるだろう。

例えば、数千万件というリストを持つ事業者に毎月リスト洗浄のためにデータを提出させるのは、容量的に運用が可能かという問題がある。もちろん、従量制の料金にしてシステムの容量を増やせばよいとも考えられるが、モデルコンプライアンスプログラム認証を受けた事業者には、毎月全部の提出というより、30 日間以内に提出した番号にのみ架電できる、というアプローチで、以後 30 日以内に架電する可能性のある番号のみを提出させるということも可能であろう。

また、書面によりテレマーケティングの同意を得て取得した情報は Do not call リストに含まれていても削除義務はないが、リスト洗浄方式でこれを実現するためには、同意を得た人の個人情報のデータベースを別に持ち、洗浄されたコールリストと合わせて使用することになる。これは、事業者にも負担になるし、チェックされない架電リストが残ることになる。従って、同意を得ている番号にはマークをつけて提出することにする。

事業者に Do not call リストにある電話番号を持たせないこと自体も意味はあるが、むしろ事業者が「運営主体」に登録した消費者の情報をもっていることを発見できる端緒となることに意味がある。そのためには、先進的な国のように、消費者が、登録しているにも関わらず電話をかけてきた事業者を Web サイトで通報できるなど、大きな負担なく通報できる仕組みとして、検知力を向上しなければならない。海外の例のように、突合しないこと自体を違法とすべきだが、このような通報でその発見も可能になり、法執行の仕組みが動き出すことができる。

もちろん、事業者には、テレマーケティングの同意を得ているかどうかの釈明の機会は与えられるべきであり、そこでもモデルコンプライアンスプログラムの認証事業者に対しては、安心して直接コンタクトできる事業者として、消費者からの直接問い合わせを義務付けてもよいのかもしれない。

リスト洗浄方式で架電リストを提出させるため、個人が申請すれば、自分の電話番号を保有する事業者のリストを参照できるサービスも可能になる[234]。そこで、利用に同意を得ているマークがついているものも含め確認でき、仮に同意をしていないのにマークがついていれば、通報するか、本人関与の原則に基づく権利行使をすることも可能である。

---

[234] 米国では、有償のクレジットモニタリングやなりすましモニタリングのサービスがあることを考えると、高くない金額で有償でもよいのではないか。

7.5.2 経済的試算

これを実現するためには、当然ながら、システムの構築や運用にも費用が掛かる。

米国が 2003 年に DNC を導入した時[235]には、「消費者による番号の登録」「業者によるリストへのアクセス」「消費者が苦情を申し立てるためのシステム」「法執行機関が参照できる登録電話番号と苦情に関するデータベース」「連邦管理のリストと州管理のリストを相互に利用可能にするためのインターフェース」の 5 つの要素がシステムに盛り込まれた。準備に当たり、FTC は米国議会から、1810 万ドルの予算を取り付けた。このうち 350 万ドルがシステム構築費用、250 万ドルが FTC のインフラをアップグレードする費用と Web サイトの再構築費用だった、とされる。

直近の DNC に特化したコストについての情報は探せなかったが、2016 年 FTC の消費者保護局全体のコストは 185 百万ドルであり、事業者から徴収したアクセス料は 14 百万ドルとなっている[236]。また、DNC が開始されて初めて年間通じて運営された 2004 年は、米国政府監査院の報告[237]によれば、DNC 制度の運営費は、システム・制度運用、執行を合わせて、表 22 のとおり、約 14 百万ドルであり、事業者のアクセス料収入は 14 百万ドル[238]で、ちょうど赤字なく運営できるようになっている。

表 22　FTC による DNC の運営コスト(発足当時)

Table 4: FTC's Costs Related to the National Registry for Fiscal Years 2003 and 2004

Cost category	Cost for fiscal year 2003	Cost for fiscal year 2004
Contract	$4,332,338	$4,339,200
Enforcement	$3,449,715	$7,282,188
Infrastructure and overhead	$12,375,012	$9,432,276
Total	**$20,157,065**	**$21,053,664**
Minus costs associated with other telemarketing sales rule efforts	$5,550,815	$7,077,409
Net total costs for national registry	**$14,606,250**	**$13,976,255**

そこで、米国にカナダ、韓国のコスト[239]から、仮説に仮説を重ねて、日本のシステム費用を

---

235 この時のシステム構築に関しては、ドラグーン・前掲注 184 に詳しい。

236 FTC, Fiscal Year 2016 Agency Financial Report, 41 頁

237 United States Government Accountability Office, Report to Congress Committees Telemarketing: Implementation of the National Do-Not-Call Registry(Jan.2005)、22 頁

238 FTC・前掲注 237、17 頁

239 米国は、本文記述の情報。カナダ、韓国は、コストは消費者庁「訪問販売・電話勧誘販売等の勧誘に関する問題についての検討③」、第 8 回特定商取引法専門調査会資料 1 (2015･7･22)より。登録数、苦情数は薬袋・前掲注 219

推計試算する。

表 23　DNC システムの試算

	米国		カナダ	韓国	日本
	2016	2004			
人口(万人)	32,000	32,000	3,585	5,062	12,706
登録数(概数　万件)	22,600	6,174	1,144	10	9,313
苦情数　(年間 万件)	534	675	9	(情報なし)	73
テレマーケター登録数(約　　)	20,000	7,100	11,000	(情報なし)	1,574
テレマーケターからのアクセス料収入	14百万ドル	14百万ドル	(情報なし)	無料	94,000
方式	リスト取得方式		リスト取得方式	リスト洗浄方式	リスト洗浄方式
構築(約　万円)		60,000	88,000	5,300	90,510
システムのみの運用(万円)		94,000	25,000	2,500	94,000

日本の登録数：電話番号数を人口数と同じと仮定。消費者庁意識調査[240]によれば、DNC ができた時に登録を希望するのは、ぜひ登録したいと手続きが面倒でなければ登録したいを合わせると 73.3%なので、人口数の 73.3%として算出。

日本の苦情数：登録数に対する比率を、個人情報保護法のあるカナダと同じ比率と仮定。

テレマーケタ数：公益社団法人日本通信販売協会[241]では、会員　475 社、有力非会員　190 社で市場規模を出しているので、いわゆる通販業者は 665 社と仮定。

米国ダイレクトマーケティング協会[242]会員数 3000 と設立当初の登録テレマーケタ数 7100 との比率から、推計

システム構築費用：米国の構築費用に、当初の登録数の比率をかけて算出。

運営費用：米国と同様と仮定。本来リスト洗浄方式の方が運営費用がかかると考えられるが、同じリスト洗浄方式の韓国において極端に低いため、米国と同様とした。

240 消費者庁、「消費者の訪問勧誘・電話勧誘・ＦＡＸ勧誘に関する意識調査」（2015 年 5 月 13 日）Q39 http://www.caa.go.jp/trade/pdf/150513kouhyou_1.pdf

241 https://www.jadma.org/pdf/2016/20160825press2015market%20size.pdf

242 http://www.dmj-inc.co.jp/dma/

この計算により、Do not call 制度の運用にかかる費用は、以下の通りとなる。

毎年の運用費用　　94,000 万円
システム構築費用　3 年償却　3 億円／年
計　12,4 億円（当初 3 年）　9.4 億円（4 年目以降）

テレマーケタからのアクセス料収入は、システム運用費をカバーするためには、単純に事業者数で割ると、年間 60 万円となり、米国のように市外局番数で傾斜をつける料金体系にすれば、事業者が支払えない金額にはならない。あるいは、もう少し高くてもよいかもしれない。言い換えれば、米国同様、運用費用は、アクセス料で賄えることになる。

一方、この制度による便益である。

DNC は基本的には消費者保護の制度である。2015 年度、刑事産業省消費者相談室が受け付けた消費者相談数[243]は 7944 件で、そのうち、電話勧誘販売関連は 453 件であった。全国の消費生活センターが受け付けた電話勧誘販売関連の相談案件は、2016 年度は 64,975 件[244]であった。仮に時給 1000 円の相談員が 30 分対応したとすると、年間 3,249 万円の損失である。また、2014 年度の電話勧誘販売関連の検挙数は 13 件、検挙人数は 60 に、被害人員は 6,944 人、被害額は 9 億 7,090 万円であった[245]。DNC が導入されて、すべての案件がなくなるわけではないが、半減はするのではないか。

また、消費者庁意識調査[246]によれば、調査時点（2015 年 3 月）までの 5 年間に、突然、電話に事業者から電話があり、商品やサービスの購入を勧められたことがあると答えた人に頻度を聞いた結果が表 24 である。

---

243 経産省『平成 27 年度における消費者相談の概況について』(2016 年 7 月)
http://www.meti.go.jp/press/2016/07/20160729004/20160729004.pdf

244 国民生活センター、PIO-NET 統計、http://www.kokusen.go.jp/soudan_topics/data/mutenpo.html

245 消費者委員会特定商取引法専門調査会　報告書（2015･12）
http://www.cao.go.jp/consumer/iinkaikouhyou/2015/doc/20151224_tokusho_houkoku1.pdf
http://www.cao.go.jp/consumer/iinkaikouhyou/2015/doc/20151224_tokusho_houkoku2.pdf

246 消費者庁・前掲注 240、Q26

表 24　電話勧誘販売の頻度

頻度（1年あたり平均）	1年換算(回)	人	のべ回数
ほぼ毎日	365	11	4,015
週に3回以上	156	53	8,268
週に１～2回	78	164	12,792
月に１～2回	18	471	8,478
半年に２～3回	5	309	1,545
年に２～3回	3	264	660
年に1回	1	131	131
ある人の合計		1,403	35,889
ある人の平均　回/年・人			25.6
ない	0	597	0
合計		2,000	35,889
平均　回/年・人			17.9

勧誘を受けない人も含めた人数をもとに、年間延べ回数から計算した一人当たり平均は17.9 回なので、平均対応時間を 5 分とすると、国民全体で、1 年間 17,945 万時間費やすことになり、時給 800 円で計算すると、1,435 億円のロスである。DNC に登録する人は、電話を受けたことがある人と思われるので、電話を受けたことがある人に限定して計算すると、一人当たり平均は 25.6 回なので、表 23 で仮定した DNC 登録人数が登録することにより、

93,134,980 人 X 約 25.6 回 X 5 分/60 分＝198,534,171 時間

年間 19,853 万時間の節約、時給換算で 1,588 億円の無駄が省けることになる。

米国の場合、2003 年、制度導入前に電話勧誘を受けた人は、一日約 1 億４００万人であった[247]。この制度を導入したブッシュ政権の 2009 年の大統領経済報告[248]によると、2007 年までにアメリカの人口の 72% がリストに登録し、そのうちの 77% が電話勧誘の数に大幅な減少がみられたと評価している。また、当該報告によると、導入後 1 年以内の調査結果として、National Do not call Registory に登録した人が 1 か月に受ける勧誘電話が 30 本から 6 本に減少したとされる。制度により、勧誘電話が皆無になるわけではないが、5 分の 1 に減少している。

これを元に計算すると、1,588 億円の無駄については、5 分の 4 の減少となるので 1,270 億円の節約となり、登録料で賄うとはいえ、年間 12.4 億円（4 年目以降は 9.4 億円）の費用とそれ以外の、対応費用や執行費用を考えても実行するメリットはあると考えられる。

[247] 上杉めぐみ・カライスコス・アントニオス「世界の勧誘規制を知る　第２回　イギリス、アメリカの Do-Not-Call 制度」国民生活 2015.7　17 頁

[248] WHITE HOUSE, ECONOMIC REPORTOF THE PRESIDENT, 2009, 244, https://georgewbush-whitehouse.archives.gov/cea/ERP_2009.pdf　(2017・8)

7.6 実質的な Do not hold へ

Do not call 制度は、架電リストからの削除までは可能だが、架電目的ではないリストまでは及ばない。Do not hold では、個人情報保護法の執行制度として具体化するにあたり、架電リスト以外に事業者が所持し取扱う情報に及ぶ必要がある。

架電リスト以外のリストを毎月 Do not call システムでチェックさせるのは現実的ではない。しかし､Do not call の苦情が多いことを端緒に個人情報保護委員会又はその権限移譲された機関による報告聴取や立入検査ができる。これによって、架電リストの元となったリストの入手経路も調査することができ、適正な取得がトレースできないものは是正勧告により削除させることも可能である。

その事業者としては適正に間接取得したつもりだったが、その流通の上流に問題がある場合もあろう。個人情報保護委員会等が調査を開始する前に、通報が複数来た段階で、事業者が入手元や取得時の確認内容を自主申告して事業者自体は違法とならない道も作ると、より違法な流通を発見しやすい。もちろん、その場合も自主的に架電リスト以外も含め、適正性が確認できないものは削除すべきである。

この時も、「運営主体」を通じて申告できるようにすれば、「運営主体」がそのデータセットの他の流通先を察知することにもつながる。

また、個人情報保護委員会は、改正法に基づくトレースにより、個人情報を利用した事業者に対し情報を提供した事業者に遡り、テレマーケティングは行わない名簿業者にもたどり着くことができるのではないか。

電話番号を含まない個人情報は Do not call では見つからない。ノルウェーやスペインのように、郵送によるダイレクトメールも対象としている国もある。リスト洗浄方式であれば、将来的に、住所や名前を拒絶リストとして登録してもプライバシー上問題はないだろう。その場合も、基本的に本人同意により直接取得している真面目な事業者に負担とならない工夫が必要だろう。

7.7 更なる発展の可能性

更に将来的には、事業者の負担を減らすためにリスト洗浄を自動的に行う仕組みも考えられるが、このためには「運営主体」のＤＢと多くの事業者のＤＢが常時接続する必要があろう。そうなれば、このような法の強制の目的だけでなく、個人向けのサービス目的にも使えるかもしれない。例えば、個人情報が取得されたことの検知や、同意を得て提供したものも含め、リアルタイムに自分の個人情報を管理するサービスにもできるかもしれない。

8　結語

個人情報保護法が施行されて、12 年。クラウド、IoT、ビッグデータの活用など、ICT の発達によるサービスの高度化に伴い、そのプライバシーとのバランスのとり方が世界で議論され、各国や地域で立法などにより規範は進化した。日本も個人情報保護法改正などで対応しようとしている。

一方で、技術の進化は攻撃技術も進化させ、攻撃ツールの流通や攻撃者の組織化などにより、漏えいを完全に防ぐことは不可能になっている。

日本における個人情報保護規範は、法ができる前から、漏えいを起こした事業者に対するレピュテーションリスクが最強の強制力であったが、漏えいした情報を扱う名簿販売事業者やそこから購入して利用する事業者には、一部の漏えいした事業者が営業秘密に基づいて地道に警告することがあるくらいで、効果的な牽制はされてこなかった。そのため、消費者は、自分の知らないところで自分の情報が流通していることを不安に思い、この不安をくみ取ったマスコミの報道もあいまって、真面目な事業者も含め、過剰反応が起こる。

本論文では、なぜ、そうなのか、消費者を守り、真面目な事業者が委縮しない合理的でフェアで実効性のある個人情報保護規範が作れないか、を、よりプラグマティックな米国と比較して考察してきた。特に、その執行状況等を、その対象事業者別に、第 1.3 節図 3 の「上流」である①本人より同意等を得て取得した事業者（当該事業者が漏えい事故を起こした場合、②漏えいした事業者ともいう）、「中流」の③名簿販売事業者などの流通事業者、「下流」の④名簿利用事業者に分けて分析した。

第 2 章では、日本の個人情報保護規範について整理した。

まず、上流②の漏えいした事業者に対する民法に基づく本人からの損害賠償については、個人情報保護法成立前に確立した、「個人の識別のための基礎的な情報」、「社会生活上、本人とかかわりのある一定範囲の者に了知される情報」であっても、「自己が欲しない他者にはみだりに開示されたくないと考えることは自然」、として、プライバシー侵害として慰謝料を認める判例が変更されていないことを確認した。

また、第 2.4.2 節では、個人情報保護法の執行状況を整理した。2005 年から 2015 年の間、強制力につながる改善勧告は、8 件しかないが、すべてが①②の本人から取得した事業者に対し、漏えい事故・事件についての改善を勧告したものであり、そのうち 6 件は、事業者が自主的に報告したか公表した事案に対し、行政処分としての報告聴取を行い、勧告を出したものである。改善勧告制度の趣旨は、「違反状態の放置により、個人の権利利益を侵害する恐れが高く、義務を履行させることを要すると、主務大臣が客観的合理的見地から判断した場合」に出すものだが、自ら報告するような事業者は当然再発防止策も計画しているはずで、勧告が必要だったかは疑問である。また、ソニー・コンピュータエンターテイメントの世界的なハッキング事件では、「個人情報保護法 33 条に基づく指導」を行い公表しているが、同条は助言しか定めていない。一方で、③漏えいした名簿を流通させた名簿販売事業者や④それを買い取った事業者には、法律上の報告聴取すら行われていない。

第 2.4.3 節では、なぜ、そのようなアンバランスな執行になったのかを調査した。その結

果、直接の原因としては、名簿販売事業者を管轄する主務大臣が決まっていなかったため、執行が行われなかった、ということが判明した。日本の個人情報保護法は、2015 年改正前は、主務大臣制をとっていた。保護法立法前から、個人情報保護が重要な金融、通信の分野では、かねてより担当官庁や業界団体がガイドラインを示し、指導をしていた。また、既にプライバシーマークによる自主規制、信用によるソフトローの規範が始まっており、その中でも、業界団体が認証機関となり業界の慣習に合わせた情報管理を普及させようという動きもあった。その中で、宇治市の漏えい事件をきっかけに個人情報保護法の立法の動きが急に始まった。個人情報保護法は企業活動や社会生活のあらゆるところに関係するため、真面目な民間企業はそれまでの慣習とは異なる規範を強制されることに警戒感があり、主務大臣制による行政法的アプローチとされることは歓迎されたと考える。しかしその結果、行政の手が届かない中小事業者や、ジャンル的にも主務大臣が明確でない名簿販売事業者などには、全く強制力がない状態に陥った。

2007 年に明らかになった個人情報の大量漏えいと漏えいした情報を使った詐欺事件を受け、同年 6 月の国民生活審議会の「個人情報保護に関する取りまとめ」でも、「市販の名簿の管理方法の検討（基本方針の見直し等又は政令改正）」が取り上げられ、2008 年 4 月 25 日付の個人情報の保護に関する基本方針改正でも、前文で「実際、事業者からの顧客情報等の大規模な流出や、個人情報の売買事件が多発し、社会問題化している。それに伴い、国民のプライバシーに関する不安も高まっており、また、安全管理をはじめとする企業の個人情報保護の取組への要請も高まっている。」とし、「各省庁が所管する分野において講ずべき施策」に「また、悪質な事業者の監督のため、個人情報取扱事業者に対する報告の徴収等の主務大臣の権限等について、これを適切に行使するなど、法等の厳格な適用を図るものとする。」とされたものの、結局、主務大臣が決められることなく、③流通事業者や④流通・流出した情報を利用する事業者に対する対策は動かなかった。

2007 年の「個人情報保護に関する取りまとめ」では、いわゆる過剰反応が問題になったこともあり、2009 年、民主党政権下で消費者庁が個人情報保護法の主管となったときも、執行は低調だった。

結果として、レピュテーションを気にする事業者が事故を起こして報告した時に執行権限が行使される以外にはほとんど強制力は行使されず、不適正な利用に関する苦情は PIO-NET に多く寄せられていたにも関わらず、主務官庁のない名簿販売事業者などの事業者は野放しであった。それは、消費者に、自分の知らないところで自分の情報が取引され利用されていることの不安を与えていた。2014 年の大量漏えい事件で、図 3 の②の事故を起こした事業者が、自身の調査の結果、持ち出された情報が名簿販売事業者を通じて流通していたことを公表し、不安が現実のものであったとして社会問題化し、初めて当該事件での流出情報についてのみ主務官庁が定められた。そして、やっと 2015 年改正に③の不適正流通や④のそれを購入した事業者による利用への対策が盛り込まれた。

このように見てくると、主務大臣制では、法の執行というよりも、自らが管轄する事業者の管理、という側面が強く、行政指導の範囲として手が及ぶ事業者は管理するが、他はしない、逆に、管理対象の事業者で漏えい事故という「不祥事」が起こり、社会問題化すると、制度の趣旨からは不要にもかかわらず改善勧告という措置を行い、社会的にも「けじめ」をつける、という行政指導的な関係だったのかもしれない、とも考えられる。

第 3 章で分析した侵害通知においても、日本は、官庁への報告が法的な義務ではないにも関わらず、ガイドラインでわざわざ微細なものとして報告不要と書かねばならないように、FAX 誤送信だけでも官庁報告がなされていた。第 5.3 節で示したように、事故の公表においても、なりすましリスクが高い情報に限っている米国と違い、すべての情報を対象にしていることもあろうが、不注意、ミスによる漏えいの開示件数も多い。このようにどんな小さな事故でも報告し通知・開示する背景には、もちろん、基本 4 情報でも民事責任を問われることや開示しないことに対するレピュテーションリスクも大きいが、行政との関係では、小さな事故でも報告することによる信頼関係の維持という行政指導文化の裏返しという面もあったかもしれない。

従って、日本の個人情報保護法の執行においては、行政指導体質から、もっと合理的で合目的的な、消費者や情報主体のための法執行へと変わらねばならない。その際、輸出管理におけるコンプライアンスプログラムのように、真面目な事業者に対しては、敵対路線ではなく対話路線で臨み、本来、取締らねばならない名簿販売事業者やその利用者に対し積極的に調査するように、メリハリをつければ、執行も合理的に行え、真面目な事業者への萎縮効果も緩和できる。

第 3 章では、個人情報漏えい事故が発生した場合に、本人に通知することにより、二次被害の防止を図る侵害通知について、日米欧の法律の状況を比較した。表 5 に示すように、米国では、なりすましのリスクのある重要な情報との組み合わせで氏名等が漏えいした場合に、本人に通知して自衛を促すことはほとんどの州で義務となっている。一部の州では、なりすまし詐欺の犯人捜査に関係するからか、州検察への報告も義務となっている。EU では、現在は電子通信プライバシー指令に基づき、通知義務があるが、2018 年 5 月から施行される GDPR でも、本人の権利と自由にリスクを与えない場合を除き、72 時間以内に監督官庁への報告が義務付けられ、また、高いリスクが発生し得る場合には本人への通知が義務付けられる。欧米とも、公表については、通知先が多く通知の負担が大きい時の代替策とされている。一方で、日本では、基本方針やガイドラインで「推奨」とされ、法的義務はないもの、どんな個人情報であっても本人通知、公表、官庁報告の三点セットが推奨されている。結果として、前述のとおり、FAX の宛先だけに個人情報が入っていた場合は報告不要、と、政府のガイドラインに書かなければいけないような真面目な運用を行う事業者がいる一方、全く行わない事業者も多い、という状況がある。本人が、漏えいしたことも知らされないなら、コントロールもしようがない。いずれ、日本でも法的な義務にすることになろうが、米国のような合理的なものにすることが望まれる。メリハリをつけ合理化した上で、義務化し、義務以上の通知を行う事業者にメリットがあり評価されるような制度にすべきである。

第 4 章では、米国の個人情報保護規範の法的枠組みとその執行状況を分析した。包括的な個人情報保護法がない米国では、連邦では政府を対象とするプライバシー法と必要に応じて業界ごとを対象とするセクトラル方式を取り、州法では主に第 3 章で取り上げた侵害通知法が運用される中、最も活発に運用されているのは FTC による調査、提訴である。プライバシーポリシーに掲げる個人情報保護や安全管理の約束が守られていない、という「欺瞞的な行為」として、FTC は無断での個人情報取得や他目的への流用、口座情報や多重債務者リスト

の流通などを取締ってきた。まさに、成文法がなくても判例の積み重ねで規範を形成するコモンローの伝統を生かしている。

第 4.4 節では、この FTC の執行状況を、その対象事業者別に、第 1.3 節図 3 の①～④に当てはめて分析した。表 10 のとおりである。そこでは、FTC は①の事業者や②のその安全管理だけでなく、③の個人情報の不適正な流通や④の不適正流通から購入して利用する事業者に対しても積極的に執行していることが分かった。特に、流通する個人情報を利用した詐欺、そこに関与するデータブローカーに力点を置いて執行している。また、第 6.2.2 節表 19 に示すように、Do not call の執行においても、自動電話による迷惑と詐欺や老人を狙った投資勧誘のような詐欺まがいの行為に力点を置いて執行しており、全体として、まさに、消費者を守るための執行を行っている。

そして、第 4.5 節で示したとおり、FTC はこれを支えるクレーム収集・検知に努力している。自らの Web サイトでも、詐欺被害につながりやすいなりすましや Do not call の通報を容易にするだけでなく、詐欺となりすましの苦情を集めるため、多くの州の検察や消費者法の執行機関、消費者金融保護局や国税局などの連邦の関連調査機関や、民間の認証団体などと、苦情情報を共有するための Consumer Sentinel Network という仕組みを通じて、苦情を集めている。そこでは、個々のクレームを取り上げるのではなく、量・質両面からトレンドを見極め、悪質なケースを訴追する、という効率的な方法を取っている。

第 5 章では、事故実績の日米比較を行った。日本は、第 3 章でみたように、侵害通知は法的義務ではないが、個人情報の種類を限定することなく本人通知、公表、官庁報告が推奨されている。この公表されたものや報道されたものを地道に集めた JNSA の事故実績を使った。米国は、第 3 章でみたように、多くの州で、なりすましや経済的被害につながる個人情報の組合せが漏えいした場合に本人通知が法的義務となっている。NY 州は同時に州検察への報告も義務付けており、こうして報告されたものを使った。

この 2 つの比較の結果、

１）外部からのシステム侵害や内部犯行など、すぐには発見しにくい内外の者による故意の窃取について、日本の件数が一桁少ない。

２）紛失置忘れや不注意、ミスによる漏えいは、少なくとも 2014 年は日本は一桁多かった。

日本では、１）の窃取の発見力が低く、むしろ、２）のような、小さな事故を真面目に公表してきた、ということが推測された。

第 6 章では、これらの分析から日米比較を行い、表 18 のように整理した。包括的な個人情報保護法がなくても、なりすましや詐欺などによる消費者被害の防止に力点を置き、③の不適正な流通や④の流通している個人情報の利用者に対しても執行を行っている米国に対し、理念先行で、消費者は知らないところで名前とコンタクト情報が流通すること自体を不安に思っているが、③の不適正流通や④の不適正利用に対しては執行も検知の仕組みもなく、漏えい事故を起こした①②の上流の事業者に対する法的対応と社会的批判に支えられている日本、というコントラストが明確になった。

その上で、第 7 章では、表 21 のように、日本における改善点として、③の不適正流通や

④の不適正利用に対する執行強化と検知強化を上げた。更に、米国と違って、なりすましや詐欺による経済的被害の防止だけでなく、「自己情報コントロール」の概念から、知らないところで名前とコンタクト情報が流通すること自体を不安に思う、日本の状況に合わせるため、米国を始め世界 18 カ国で採用されている Do not call を利用した検知を行うことを提案した。

まず、第 7.3 節では、2015 年改正法を十分活用し、米国のように、PIO-NET を活用して、④の不適正利用に関する苦情を検知し、クレームが多い事業者や悪質な事業者を中心に調査をし、③の名簿販売事業者への執行を強化することを提案した。これによって、消費者の不安を減少させることができる。

更に第 7.4 節以降では、創造的な制度として、外郭団体を活用した 2 つの制度を提案した。

2015 年改正において委員会の Web サイトに掲出されることとなった比較的遵法意識のある名簿販売事業者に対してでさえ、自分の情報を持っているかどうかの開示を求めるには、勇気も手間も必要である。下手に開示請求をして、本人確認資料を求められれば、更なる情報を提供せざるを得ず、それがまた販売されないとは限らないからである。そこで、信頼できる団体を作って、これを本人確認情報を相手に提供せずに代理させることを提案した。これにより、削除請求などの本人関与原則を安心して行使できる。

更に、第 7.5 節では、世界 18 カ国で導入されている Do not call 制度が日本に導入される際には、それを不正利用の検知ツールとし、そこから遡って、架電リスト以外のデータも削除させられるようにすることを提案した。

このように整えていけば、消費者は Do not call の「運営主体」に登録するだけで、同意しない事業者にコンタクトすることなく自らの個人情報を削除させ、執行機関は違法に取得する事業者を発見でき効果的な執行の端緒とできる。

これにより、消費者と真面目な事業者に過剰な負担を負わせず、保護と活用のバランスが取れ、悪質な事業者に対する発見と積極的な調査により不正な流通を取り締ることで、事業者全体にバランスのとれた実効性のある制度や運用となる。そして、不適正流通事業者や不適正利用事業者への取締り強化により、消費者の不安を減少し、委員会が悪い事業者を取締ってくれるという信頼の下、安心して活用にも同意できるようになり、情報化社会の進展と消費者や社会が安心してそれを享受できる社会を作ることができよう。

参考文献　（五十音順）

アリス･ドラグーン「DO NOT CALL REGISTRY わずか 100 日で電話セールス撲滅システムを構築した米国連邦取引委員会」CIO : Business technology leadership 5(12), 90-99, 2004-12
石井夏生利『新版　個人情報保護法の現在と未来　世界的潮流と日本の将来像』（勁草書房, 2017 年）
大島義則他、『消費者行政法』（勁草書房、2016）
岡村久道『個人情報保護法〔新訂版〕』（商事法務、2009 年）
岡村久道＝新保史生『電子ネットワークと個人情報保護－オンラインプライバシー法入門―』（経済産業調査会、2002）
小向太郎「米国 FTC における消費者プライバシー政策の動向」情報通信政策レビュー第 8 号(2014 年)
佐々木秀智「最近の判例　最近の判例 Mainstream Marketing Services, Inc. v. Federal Trade Commission, 358 F.3d 1228 (10th Cir.), cert. denied, 543 U.S. 812 (2004)--迷惑な商業テレマーケティングを規制する Do-Not-Call Registry は,プライバシーおよび消費者保護を目的とした,テレマーケティング業者の営利的表現の自由を必要以上に制約しない合理的な規制であり,合衆国憲法第 1 修正に違反しない」アメリカ法　2006(2), 365-371
日置巴美＝板倉陽一郎『個人情報保護法のしくみ』（商事法務，2017）
薬袋 真司ほか「世界の勧誘規制を知る」　『国民生活』2015 年 6 月号～2016 年 7 月号(2015～2016)(2017.2)
湯淺墾道「アメリカにおける個人情報漏洩通知法制に関する考察」情報ネットワーク・ローレビュー第 11 巻(2012 年 11 月)72-87

Daniel J. Solove & Woodrow Hartzog, The FTC and the New Common Law of Privacy , COLUMBIA LAW REVIEW [Vol. 114:5839](2013)
INFORMATION SECURITY AND PRIVACY, A PTACTICAL GUIDE FOR CLOBAL EXECUTIVES, LAWYERS AND TECHNOLOGISTS (Thomas J. Shaw Esq. Ed., 2011)

その他の文献は脚注を参照