

アメリカにおける個人情報漏えいの被害者保護に関する新たな動き (1)

——原状回復法による保護をめぐる議論を中心に——

橋 本 伸

I 序——問題の所在

- (1) 概説
- (2) 日米における個人情報漏えい問題の対応状況
- (3) 日米における現状に対する批判
- (4) 本稿の目的と叙述の構成

II 従前の個人情報漏えいの被害者保護の問題点

- (1) 概説
- (2) 手続法上の問題——憲法上の「原告適格」の障害
- (3) 実体法上の問題①——不法行為に基づく請求の障害
- (4) 実体法上の問題②——契約違反に基づく請求の障害
- (5) 従来 of 状況の原因とそれに対する疑問
- (6) 小括 (以上, 本号)

I 序——問題の所在

(1) 概説

近年, 企業が保有する顧客の個人情報漏えい (流出)¹⁾ する事件が多発し

1) 用語法について一言述べておく。「漏えい」は, 過失による場合を, 「流出」は, 故意による場合を想定して, 両者を分けて用いる理解もある (板倉陽一郎「従業者等による個人情報の流出と対策」法律のひろば 69 巻 5 号 (2016) 38 頁) が, ア

ていることは周知の通りである²⁾。このような個人情報の漏えいが生じる場合としては、①従業員の紛失・誤操作による場合、②サイバーアタックやハッカーによる不正アクセスを受けた場合、③(転売等の目的のために)従業員により持ち出された場合、④(③の従業員等から入手した)名簿業者が当該情報を必要としている企業等に売却した場合、⑤企業が顧客の事前の同意を得ることなしに取得した個人情報を営利目的で第三者に売却した場合などが考えられる³⁾。このような個人情報の漏えいは、顧客にプライバシーに関わる個人情報が悪用されるリスクをもたらしめている⁴⁾。このことは、アメリカにおいて、不正に入手した他者の個人情報を悪用して、銀行口座やクレジットカード等の作成や不正利用、医療サービスの不正受給等を行う犯罪行為(いわゆる「ID窃盗(identity theft)」)が、急速に増加しており、大きな社会問題となっていることから明らかであろう⁵⁾。

アメリカでは“data breach”として区別せず用いられていることに鑑み、本稿では、「漏えい」で統一して用いる。

- 2) わが国における個人情報漏えいに関する民事上の責任問題全般に関しては、さしあたり、西村あさひ法律事務所編『個人情報保護法制大全』(商事法務, 2020) 341-379頁, 牛丸達夫「情報漏えいと企業の民事責任」近大法学 69巻 1=2=3号(2021) 25頁以下を参照。
- 3) 新聞報道等の個人情報流出事例を集計した報告書によれば、「紛失・置忘れ」、「誤操作」、「不正アクセス」の3つのタイプで個人情報漏えいの7割近くが占められているとされる(この点については、NPO日本ネットワークセキュリティ境界「2018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～(速報版)」(2019)を参照。この報告書は、同協会のホームページから入手可能である(<https://www.jnsa.org/result/incident/2018.html>)。最終閲覧:令和5年4月2日)。
- 4) 石井孝明「米国におけるサイバーセキュリティ関連法制の一考察——データ情報漏えいを取り巻く法的責任について」NBL1139号(2019) 28頁。
- 5) DANIEL J. SOLOVE & PAUL M. SCHWARTZ, CONSUMER PRIVACY AND DATA PROTECTION (3rd ed.) (Aspen Pub., 2020) 114。その規模については、漏えいした個人情報の4分の1がID窃盗等の不正な目的に利用されているというデータの存在も指摘されている(*Id.* at 344)。この点につき、松前恵環「米国個人情報・プライバシー保護法制をつかむ(第6回)個人情報の保有及び管理に関する規制」NBL1195号(2021) 80頁以下、特に81頁注(3)および85頁注(71)を参照。なお、ID窃盗一般については、高月昭年「なりすまし犯罪の急増と米議会の対応」国際金融 1104号(2003) 28頁以下、中川かおり「米国における個人情報保護の動向——個人情報窃盗対策を中心に」外国の立法 231号(2007) 59頁以下も参照。

ところで、このような自己の個人情報が漏えいされた場合、その後には詐欺などによって、現実の損害を被った場合はともかく、そこにまで至っていない段階（すなわち、不快感や不安感を抱いているに過ぎない段階）において、個人情報が漏えいされた顧客（被害者）は自己の情報を漏えいした企業等（加害者）に対して損害賠償請求することができるのであろうか。この問題について、日米において、対照的な状況となっていることが興味深い。そこで、以下では、本稿の問題意識を明らかにするためにも、この問題につき日米でどのような法的な取扱いがなされているかについて確認していくことにしよう。

(2) 日米における個人情報漏えい問題の対応状況

結論を予告的に述べておくと、日米における対照的な取扱いの主たる原因は、「損害」要件の認定につき両国におけるスタンスの相違という点にあるように思われる。すなわち、アメリカでは、個人情報漏えいの場面において被害者の「損害」を認定するのに消極的な傾向があるのに対し、日本では、それを認めることに抵抗が少ないということである。以下では、この点について両国の状況を順に見ていくこととする。

(i) 日本法

わが国では、個人情報を本人の承諾なしに第三者に提供した事案において、判例は、具体的不利益を考慮することなしに、被害者に精神的損害の賠償を認めてきた⁶⁾。このような理解を推し進めると、個人情報の漏えいの事案においても、現実の損害を被っていない段階であっても、それのみをもって直ちに「損害」要件の充足が否定されることにはならないであろう。もっとも、この点につき、近時のベネッセの個人情報漏えい事件⁷⁾において問題となった。

6) 最判平 15 年 9 月 12 日民集 57 卷 8 号 973 頁。

7) 最判平 29 年 10 月 23 日判時 2351 号 7 頁。同判決の評釈・解説としては、高松志直・NBL1109 号 (2017) 21 頁以下、山下純司・法教 449 号 (2018) 123 頁、影島広泰・ビジネス法務 18 卷 4 号 (2018) 74 頁以下、加藤新太郎・NBL1127 号 (2018) 96 頁以下、中山布紗・立命館法学 380 号 (2018) 259 頁以下、千葉恵美子・平成 29

本件は、大手通信教育会社ベネッセコーポレーション（Y）の業務委託会社から最大2070万件の氏名、住所、生年月日、メールアドレス等の個人識別情報の漏えいがあったことが公表され、被害者XらがYに対して民法709条に基づき損害賠償請求したという事案である。

本件では、原審と最高裁において「損害」要件の充足の有無をめぐって理解が分かれた。すなわち、原審⁸⁾は、「自己の氏名、郵便番号、住所、電話番号及びその家族である者の氏名、性別、生年月日が名簿業者に売却されて漏えいすると、通常人の一般的な感覚に照らして、不快感のみならず、不安を抱くことがあるものと認められる。／しかし、そのような不快感や不安を抱いただけでは、これを被侵害利益として、直ちに損害賠償を求めることはできないと解するのが相当である。／本件においては、本件漏えいによって、Xが迷惑行為を受けているとか、財産的な被害を被ったなど、上記の不快感や不安を超える損害を被ったことについて主張、立証はない。」として、「損害」要件の充足において金銭的な損害等の具体的な損害の発生を要求して、不法行為の成立を否定した。

これに対し、最高裁は、「原審は、上記のプライバシーの侵害によるXの精神的損害の有無及びその程度等について十分に審理することなく、不快感等を超える損害の発生についての主張、立証がされていないということのみから直ちにXの請求を棄却すべきものとしたものである。そうすると、原審の判断には、不法行為における損害に関する法令の解釈適用を誤った結果、上記の点について審理を尽くさなかった違法があるといわざるを得ない。」と判示した。もちろん、このような判決文からは、直ちに「損害」要件につき最高裁自身がどのような立場を採るかは明らかではないものの⁹⁾、少なくとも原審判決と比

年度重要判例解説（ジュリ臨増1518号）77頁以下（2018）、水野謙・リマークス58号（2019）30頁以下、始澤真純・現代社会研究（東洋大学）17号（2020）123頁以下、千手崇史・商経学叢（近畿大学）66巻1号（2019）259頁以下、神作裕之・消費者法判例百選（第2版）（別ジュリ249号）249頁以下（2020）などがある。

8) 大阪高裁平28年6月29日判時2351号9頁。

9) 判タ1442号47頁（匿名コメント）。同旨、加藤・前掲注（7）99頁。

較すると、被害者の救済可能性を大きく切り開いた判決であるとの積極的な評価がなされている¹⁰⁾。

そして、その後の差戻審¹¹⁾は、「個人情報が外部に漏えいしてプライバシーが侵害された場合に、当該被漏えい者が精神的苦痛を被ったか否か及び被った精神的損害を慰藉するに相当な額を検討するに当たっては、流出した個人情報の内容、流出した範囲、実害の有無、個人情報を管理していた者による対応措置の内容等、本件において顕れた事情を総合的に考慮して判断すべきである。」と述べた上で、本件のXらの個人情報が漏えいしたものの、具体的に名簿利用による勧誘や電話により日常生活に支障を及ぼすなどの実害は発生した場合のみならず、それが生じていない場合でも「個人情報を利用する他人の範囲を自らコントロールできない事態が生じていること自体が具体的な損害」に当たるとして、「損害」を認定しつつ、Yの誠実な事後対応を踏まえると、1000円の賠償額を相当とした。もちろん、上記の判断枠組みを前提としたとしても、それらの認定において具体的にどのような事情を考慮するかについて、裁判官によって理解が異なることはあり得るであろう¹²⁾。しかし、従前の判例の流れを推し進めれば、わが国では、本件のような大規模な情報漏えい事件において、現実的損害が発生しておらず、不快感や不安を抱くにとどまる段階でも、それのみをもって直ちに「損害」がないとして、請求が当然に遮断されることにはならないであろう（ただし、その代わりとしてか、最高裁は、個人情報漏えいの事案においては、従前の先例とは異なり、権利ないし法益侵害とは別に、「過

10) 神作・前掲注(7) 248頁。その他、損害論について同旨の評価として、中山・前掲注(7) 279頁（最高裁は個人情報の漏えいによる二次被害の損害が現実には発生せず、不安感のみを抱いた場合であっても損害を認定できる可能性があるという立場を明らかにしたと評価する）、牛丸・前掲注(1) 63頁（率直に解釈すると、単なる不安感しか被っていない場合であっても、損害賠償が認められるべきことを示したと指摘する）がある。

11) 大阪高判令元年11月20日判時2448号28頁。

12) 現に、ベネッセ関連のその他の訴訟においては、「損害」の認定について上記の判断枠組みを採りつつ、結論として「損害」を否定した裁判例もある（東京地判平30年6月20日判時2440号45頁。ただし、上訴審である東京高判令元年6月27日判時2440号39頁は肯定している）。

失」要件を問題としている¹³⁾ 14)。

(ii) アメリカ法

これに対し、アメリカでは、個人情報の漏えいがあっても、被害者が現実の損害を被っていない段階では、「損害」要件が充足されないために、損害賠償は認められない傾向がある¹⁵⁾。

その理由としては、——詳細は後述するが——個人情報が漏えいの場面では、被害者が、例えばコモン・ロー上の過失による不法行為を理由に損害賠償請求する場合、その要件として「損害」を被っていることが必要となるが、上記の場面で生じる精神的な損害はここでの「損害」に含まれないと解されていること、また、連邦裁判所に管轄が属する場合には、被害者は合衆国憲法上の「原告適格 (standing)」要件の障害があり、その要素の一つとして、損害が現実的なものであることが求められているが、上記場面では現実的なものと解されないことなどが挙げられる。

このようにアメリカでは、「損害」要件が障害となって、被害者の救済は制限される傾向があるといえる。もちろん、こうした状況は、後述するように、アメリカでは、個人情報の保護は、私的執行 (private enforcement) ではなく、

13) この点につき、本件のようなサイバーセキュリティが問題となる事案類型においては、過失を独自の要件として位置づけることについて積極的に評価する見解も見られる (角本和理「サイバー時代におけるプライバシーの法理論 (7・完) ——私法上の問題を中心に」北法71巻4号(2020) [1] 頁, 特に [41] 頁以下を参照)。

14) わが国の判例・学説が、個人情報の誤用 (漏えい) の場面において損害賠償を比較的容易に認める傾向があるという点につき、加藤隆之「個人情報の誤用に起因する損害の発生と賠償額の算定」亜細亜法学54巻2号(2020) 1頁, 特に9頁の指摘も参照。

15) わが国におけるアメリカの個人情報漏えい問題に関する先行研究として、中川・前掲注(5) 59頁以下、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号(2017) 133頁以下、佐々木秀智「アメリカ不法行為法における個人情報漏えいの『損害』について」法律論叢91巻2=3号(2018) 91頁以下、石井・前掲注(4) 28頁以下、松前・前掲注(5) 80頁以下、牛丸達夫「米国における情報漏えいと企業の法的責任——Information Fiduciariesに関する議論を中心に」近大法学70巻1号(2022) 179頁以下などがある。

行政機関による公的執行 (public enforcement) に委ねられており、上記の状況をもって直ちに漏えいした企業等が何らの責任に服さないことを意味するわけではないが、少なくとも被害者自身が自己の権利を実現する手段は制限されているといえよう。

(3) 日米における現状に対する批判

ともあれ、このように日米の現状は、私的執行による個人情報漏えいの被害者保護について対照的な立場を示しているといえる¹⁶⁾。もっとも、両国においてこうした立場が何ら異論なく受け入れられているわけではない。以下では、そうした批判的な学説の立場について見ていくことにしたい。

(i) 日本法

まず日本の学説についてみると、個人情報漏えいの事案において現実の損害を被っていない段階において、被害者に損害賠償請求を認めることについては、肯定する見解も多いが¹⁷⁾、疑問を提起する見解も見られる。後者の見解につい

16) このような相違は、漏えいした情報の性質の違いも考慮すると、より顕著である。すなわち、アメリカでは、機微性が比較的高い情報 (社会保障番号やクレジットカード番号など) が漏えいした場合でも、被害者の救済は認められにくいのに対し、わが国では、機微性が高い情報が含まれる場合はもちろん、比較的低い情報 (名前、性別、住所、電話番号など) のみが漏えいした場合でも、認められる傾向がある。

17) 例えば、佐々木・前掲注 (15) 125 頁以下 (下級審裁判例が個人情報漏えいの事案において、実損害の主張・立証を要求することに対し、アメリカの個別法の判例の立場との類似性を指摘しつつも、早稲田大学名簿提出事件判決や個人情報保護法 3 条において人格的な利益の保護の間から個人情報の法的保護の前提が構築されていることを踏まえると、そうした立場を日本法において採用する必要はないとする。ただし、1000 円程度の賠償額では不十分であるとする)、角本・前掲注 (13) [50]-[51] 頁 (ベネッセ個人情報漏えい事件を含む、近時の判例の傾向として、個人に関する様々な情報が多角的に利活用される社会においては、自身に関わる情報が蓄積されるデータベースに高度な情報セキュリティが施されることを期待し、適切な情報管理がなされるであろうことを信頼することが、個人単位でみて被害が重大であるか否かにかかわらず許されていると評価できると指摘する) など。その他、結論として、最高裁の立場を支持するものとして、千手・前掲注 (7) 264 頁、始澤・前掲注 (7) 128 頁 (顧客の情報が漏えいされた不安や、ダイレクトメール・勧誘が多発した不快について、慰謝料請求が認められた本判決を妥当とする)。

て整理すると次の通りである。

第1に、比較法的な状況からわが国の立場の異質性を説くものである¹⁸⁾。この立場は、先述のアメリカの判例の立場を踏まえて、個人情報漏えいの場面において比較的容易に「損害」を認めるわが国の立場を批判的に見ている。しかも、こうした理解は、ベネッセ個人情報漏えいに関する下級審の裁判例の中でも見られる。すなわち、「なお、現代社会においては、企業等の法人や国、地方自治体等が大量の個人情報を保有することは珍しくなく、これらの個人情報が大量に流出する事態は、近年、我が国だけでなく、諸外国においても相当数発生しており、その中には、個人情報を保有していた主体が所在する国だけではなく、他の国に居住している顧客の個人情報が流出している事例もあるところ(公知の事実)、米国、英国、フランス及びドイツのいわゆる先進国等においては、本件のように主に個人識別情報が流出しただけでなく、クレジットカード番号等も流出したような事例(個人情報が第三者に悪用される可能性が高く、現実的な被害が発生する危険性は、主に個人識別情報が流出した場合に比べて、格段に大きいと考えられる。)を含め、これまでに個人情報が流出したということだけで損害賠償を命じた裁判例は見当たらない」と述べられており¹⁹⁾、日本法の特異性がより明確に指摘されているといえる。

もちろん、こうした理解に対しては、他国がそうであるからといって当然にわが国も同様に解さなければいけない理由はないとする反論が直ちに提起されるであろう²⁰⁾。そのため、より実質的な理由が問われなければならない。それが以下の点である。

第2に、被害者に損害賠償を認める実質的根拠が不十分であるとする。例え

なお、その後の下級審における肯定例を支持するものとして、前田太郎「判批(東京高判令和元年6月27日)」現代消費者法50号(2021)97頁、特に105頁(上記判決の精神的苦痛および慰謝料に関するそれぞれの判断を支持する)も参照。

18) 例えば、佐藤・前掲注(15)138頁(情報流出のあらゆる事例においてプライバシー侵害を理由とする損害賠償を認めることは、必ずしも適切ではないと指摘する)。

19) 東京地判平30年6月20日判時2440号45頁。

20) 佐々木・前掲注(15)125頁以下。

ば、このような場面において損害を肯定する見解は、具体例としてオンライン上の行動ターゲティング広告を挙げ、その根拠の一つとして、そのような広告が個人の判断の幅を狭め、自律性を害することになるという点を挙げるが、「こうした情報提供に応じるか否かは、個人に選択権があり、それがありがたいと思う個人もいるであろうから、必ずしも個人にとって不利益とはいえないように思われる。」として、その説得力がないことを指摘する²¹⁾。

第3に、損害賠償を認めることによる弊害という点から説明するものもある。この点は大きく二つに分けることができる。一つは、ベネッセ個人情報漏えい事件のようにプライバシーに関わるリスクが抽象的に増大したにとどまる事案では、裁判所が慰謝料請求を広く薄く認容することは損害の予防に資する側面がないとはいえないとしつつも、そのような慰謝料は、企業の経営を悪化させ、また個人情報の流出の隠蔽にもつながりかねないなどマイナスの側面の方が大きいとして、むしろ予防措置や情報漏えい後の対策を事業者に適切にとらせることの方が重要であると指摘するものである²²⁾。もう一つは、個人情報の漏えいの場面において財産的損害を伴わない場合には、容易に損害を認めると他者の情報利用行為を著しく阻害するという効果をもたらすことになりかねないとして、精神的損害の発生の有無については慎重に判断するべきと指摘するものである²³⁾。これらの立場は、損害賠償を広く認めることにより生じる弊害を懸念して、否定的な立場を採っているといえる。

21) 加藤・前掲注(14) 54頁以下。なお、加藤は、個人情報漏えいにより損害賠償が全く認められないと述べているわけではない。すなわち、「肯定されるためには、情報が機微なものであること、または、当該情報の誤用について個人的な関わり合いが少なくとも必要である。」と述べる(61頁)。

22) 水野・前掲注(7) 33頁。なお、中山・前掲注(7) 279頁(従来の先例と異なり、権利ないし法益侵害と過失判断を切り離して二元的に判断されていることから、不法行為が容易に成立しやすくなり、今後個人情報の漏えいに係る訴訟の頻発が危惧されるとして、原審判決のような不快感や不安を超える損害が認定される立場の方が妥当であると指摘する)、加藤・前掲注(14) 63頁(たったひとつの些細な個人情報の取扱いに関する事故で、倒産という危機に直面することになりかねないと指摘する)も同様の懸念を示していると思われる。

23) 加藤・前掲注(14) 53頁。

第4に、——必ずしも個人情報漏えい問題のみを念頭に置いて論じるものではないが——わが国においてプライバシー概念が広く認められることによって、不法行為の成立を制限する機能（スクリーニング機能）が弱まっているとして、権利侵害以外の要件（例えば、損害）にこのような機能を求める必要性を指摘する立場もある²⁴⁾。このような理解によれば、損害は、賠償対象となるものと対象とならないものに大別されることになる。

このように、消極的な見解は、個人情報漏えいの場面において「損害」を認めるのに消極的な理由として、比較法的状況、実質論（被害者のために肯定する積極的な理論的根拠の不十分性と肯定することによる加害者への弊害の大きさ）、不法行為責任のスクリーニング機能といった点を挙げているといえよう。

(ii) アメリカ法

次に、アメリカの学説について見ると、先述の個人情報漏えいの被害者に対する消極的な判例の対応状況を批判し、個人情報漏えいは、今日のデータ社会においては、被害者のその後の生活に大きな影響を及ぼすことがあることから、漏えい段階の精神的苦痛を理由に「損害」要件の充足を認めるべきと説く見解が複数提案されている²⁵⁾。

例えば、ある見解は、個人情報漏えいの場面では、リスク（個人情報詐欺や窃盗などに用いられること）や不安（被害者が将来の損害のリスク増加について不安を感じること）を理由に損害を認定することに消極的な多数の判例の立場に対して、他の場面において用いられる「確率的損害（probabilistic

24) 例えば、道垣内弘人ほか「慰謝料をめぐる問題——慰謝料はどのような場合に発生するか」論ジュリ 27号（2018）134-5頁（道垣内発言）。なお、個人情報漏えいとの関係でも同様の指摘をするものとして、木村和成「判批（東京高判令和元年6月27日）」新・判例解説 Watch26号（2020）70頁以下（損害要件にスクリーニング機能をもたらせることも一考に値すると指摘する）がある。

25) E.g. M. Ryan Calo, *The Boundaries of Privacy Harms*, 86 IND. L.J. 1131, 1132-25 (2011); Daniel J. Solove & Danielle Keats Citron, *Risk and Anxiety: A Theory of Data-Breach Harms*, 96 TEX. L. REV. 737, 785 (2018); Peter Ormerod, *Making Privacy Injuries Concrete*, 79 WASH. & LEE L. REV. 101 (2022).

injuries)」を上記場面にも拡張することにより、「損害」要件の充足が認められると説く。その根拠としては以下が挙げられる。

第1に、リスクを理由に損害を認定する根拠として、①濫用されるまでには何カ月または何年もかかるが、一度利用されると、損害は深刻になり得ること²⁶⁾、②重要な生活活動に従事する人の能力に委縮をもたらすこと（例えば、家の購入、雇用など）²⁷⁾、③リスクを認識可能な損害として承認するための基礎が法には存在すること（例えば、医療過誤や環境法など）、そしてデータ侵害もリスクが明白に終わりが見えない点で他の場面と類似するため、類推できること²⁸⁾を挙げる。

第2に、不安を理由に損害を認定する根拠として、①侵害された情報の犯罪利用を予防する手段が存在しないこと（信用監視は事後的な異常を知らせるにとどまること）²⁹⁾、②犯罪者は何時でも被害者を騙すために、その情報を使用することができること³⁰⁾、③被害者の個人情報、彼らの財政破綻をもたらすことができる犯罪者の手許にあるという事実について不安を感じることは合理的であること³¹⁾、④一定の個人情報（例えば、社会保障番号）については適切な対策（例えば、シュレッダーにかけること）が要請されるが、合理的な人はこれらの対策が有害なことが起こるのを防ぐためだと考えること³²⁾、⑤慢性の病気にかかる不安を理由に損害として承認する先例（例えば、エイズにかかる可能性やアスベストに曝露した後のガンにかかる可能性を理由とする精神的苦痛）が存在しており、ここでの場面に類推できること（というのも、ID窃盗のリスクへの曝露は、時間と金銭を伴う個人の生活への影響を伴うからである）³³⁾を挙げる。

26) Solove & Citron, *supra* note 25, at 756.

27) *Id.* at 759.

28) *Id.* at 760.

29) *Id.* at 765.

30) *Id.* at 766.

31) *Ibid.*

32) *Id.* at 767.

33) *Id.* at 772.

このように、肯定する見解は、個人情報漏えいの場面において被害者に生じるリスクや不安を個人が抱く主観的感情以上のものであることを指摘することにより、「損害」を根拠付けようとしているといえる。

(4) 本稿の目的と叙述の構成

このように日米の法状況は、一見すると、対照的な立場を示しているように見えるものの、その後の学説の議論状況まで踏まえると、この問題の解決のあり方をめぐっては、いまだ検討の余地が残されているといえよう。もっとも、上記の立場にはいずれも一長一短な点もあることを踏まえると、それらとは異なる観点から考察することも必要であろう。

そのような中で本稿が目指すのは、アメリカにおいて「損害」要件を柔軟に解する立場と同様に、判例の消極的な立場を批判しつつも、それとは異なる観点からアプローチする立場がある。それは、原状回復法——詳細は後述するが、簡単に言えば、わが国の不当利得法に相当する法領域である——により個人情報漏えいの被害者の救済を図ろうとする立場である。この立場は、冒頭で挙げた個人情報の漏えいの発生原因のうち、②や③の場面では、企業が求められる（あるいはプライバシーポリシーで約束した）水準のセキュリティ措置を採らなかったことにより生じた場合には、それにより節約した利益が、また④や⑤の場面には、個人情報を売却したことによる利益があることに注目し、(被害者に生じた「損害」ではなく)加害者に生じた「利益」に着目する形で被害者救済を図ろうとするものである³⁴⁾。

34) 本稿は、こうした原状回復法による保護を志向する立場をアメリカにおける個人情報漏えいの被害者保護に関する「新たな動き」として捉えたものの、学説の多数は、先述の「損害」要件を正面から乗り越えることを目指しており(See, Caprice Roberts, *Wrongful Gains from Data Breaches*, 2020 JOTWELL: J. THINGS WE LIKE 1, at para.3 (2020)), 原状回復法を用いて「損害」を迂回しようとする立場は現段階では少数説にとどまっている。その意味で、両者を並列的に捉えることには躊躇を覚えるところであるが、後述のように「損害」要件を正面から乗り越える立場にも、問題はあり、またプライバシー権の保護にとって原状回復法を用いる手法は、一定の意義(とりわけ、後述のように、原状回復救済を通じた新たな権利の創設の可能性を示唆する点)があると考え、このように位置づけておくことにしたい。

本稿は、このような原状回復法により保護を志向する近時の見解を主として取り上げ、このような手法が個人情報漏えいの被害者保護にとっていかなる意味を持っているのかについて若干の検討を行うことを目的とする³⁵⁾。その際に、本稿は、原状回復法による保護を提案する近時の学説として、ローレン・ショルツ (Lauren Henry Scholz)³⁶⁾ とバーナード・チャオ (Bernard Chao)³⁷⁾ の見解を中心に考察を加えることとする³⁸⁾。その理由としては、両者がこの問題についてある程度まとまった形で論じている数少ない論者であることに加えて、以下の理由を挙げることができる。すなわち、

第1に、両者の見解は、個人情報漏えい訴訟に付随する「損害」要件の障害を回避するために、原状回復法を利用することを提案することに加えて、より

35) その主観的な事情としては、筆者がこれまで英米の原状回復法、とりわけ、利益吐き出し救済に関心を持っていることに加えて、前稿において、プライバシー侵害による利益吐き出しの問題も取り上げたが、その際に、個人情報漏えいの問題については考察の対象としなかったためである。その意味で、本稿は、前稿の補論を兼ねるものでもある。

36) ショルツの見解については、Lauren Henry Scholz, *Privacy Remedies*, 94 IND. L. J. 653 (2019) (Scholz ①で引用) を参照。なお、Scholz のプライバシーの法的性質の理解については、do., *Privacy as Quasi-Property*, 101 IOWA L. REV. 1113 (2016) (Scholz ②で引用) (排他的な関係の権利 (準財産権とする) と捉える立場を採る)、またプライバシー権を保護するための手段として私的執行の役割については、do., *Private Rights of Action in Privacy Law*, 63 WILLIAM & MARY L. REV. 1639 (2022) (Scholz ③で引用) (公的執行を補充するものとして、私的執行の役割の重要性を説く) を参照。

37) チャオの見解については、Bernard Chao, *Privacy Losses as Wrongful Gains*, 106 IOWA L. REV. 555 (2021) (Chao ①で引用) ; do., *Unjust Enrichment: Standing Up For Privacy Rights*, _ IOWA L. REV. ONLINE _ (forthcoming) (参照は SSRN 版による) (Chao ②で引用) を参照。なお、前者の論稿については、原状回復法研究者 (とりわけ、契約違反による利益吐き出しを専門とする) でもある Roberts, *supra* note 34 のコメント (チャオの個人情報漏えいの被害者のために原状回復法を利用する提案を肯定的に評価する) がある。

38) その他の原状回復法による保護を志向する立場として、Lior Jacob Strahilevitz, *Data Security's Unjust Enrichment Theory*, 87 U. CHI. L. REV. 2477 (2020) もあるが、同論文については、角本和理「論文紹介『データセキュリティの不当利得理論 Lior Jacob Strahilevitz, *Data Security's Unjust Enrichment Theory*, 87 U. CHI. L. REV. 2477-2491 (2020)』」アメリカ法 2021 (2) 号 (2022) 297 頁以下で既に紹介されているので、本稿では取り上げない。

積極的に原状回復法による保護がプライバシー権の保護にとって望ましいとの考え方を提案するものであるからである。

第2に、両者の見解は、念頭においている個人情報漏えいの場面に違いがあるためである³⁹⁾。すなわち、ショルツは、データ主体（被害者）と漏えい者との間に何らかの契約関係がない場面（具体的には、データブローカーによる取引の場面）を念頭に置くのに対し、チャオは、両者の間に何らかの契約関係がある場면을念頭に置いている⁴⁰⁾。これらの二人の見解を取り上げることで、個人情報漏えいの場면을広く考察対象とすることが可能になるといえよう。

以上の理由から本稿はこれらの見解に若干立ち入って考察することとする⁴¹⁾。

39) See, Chao ①, *supra* note 37 at 572.

40) こうした区別については、Sharkey, *infra* note 81（データセキュリティの場面における被害者救済を当事者パラダイムと非当事者パラダイムに分けて損害要件についての考察を加える）も参照。なお、ベネッセ個人情報漏えい事件でも、漏えいした情報には、同社の顧客（会員）情報のほか、子ども向けスタンプラリーで収集した非会員の個人情報が含まれていた（この点につき、城田真琴『パーソナルデータの衝撃——一生を丸裸にされる「情報経済」が始まった』（ダイヤモンド社、2015）32頁以下参照）。

41) なお、直接的には原状回復法による保護を提案することを意図しているわけではないかもしれないが、原状回復救済（とりわけ、利益吐き出し）を認めることを理論上可能にする点で同一の系譜にあると思われるアメリカ法の議論がいくつかある。ここではそれらについて簡単に紹介しつつ、本稿で取り上げる原状回復法に関する議論を別途取り上げる必要があることについて簡単に言及しておきたい。

第1に、個人情報を管理する者に信認義務を課し、受認者として扱うことを試みる議論である（情報受認者に関する議論については、既にわが国でも紹介されているため、詳細はそちらに譲る。例えば、齊藤邦史「信認義務としてのプライバシー保護」情報通信学会誌 36巻2号（2018）127頁以下、村上康二郎「プライバシー権に関する信認義務説と多元的根拠論」情報ネットワーク・ローレビュー 21号（2022）28頁以下など）。というのも、信認義務違反は、従来、エクイティの排他的管轄権が認められてきた領域でもあり（See, Samuel L. Bray, *Remedies*, in: ANDREW GOLD ET AL. EDs., OXFORD HANDBOOK OF NEW PRIVATE LAW (Oxford U.P., 2021) 563, 570), 利益吐き出しが最も広く認められており、個人情報を管理する者を受認者として扱うことは、こうした救済を認める余地を生むからである。こうした可能性は、本稿が目指す原状回復法による保護を志向する見解（Chao ①, *supra* note 37, at 601-2; Lauren Henry Scholz, *Fiduciary Boilerplate: Locating Fiduciary Relationships in Information Age Consumer Transactions*, 46 J. CORP. L. 143, 146 (2020)）のみならず、信認義務違反構成を説く見解においても示唆されている（例えば、牛丸・前掲注（15）218頁の指摘〔忠実義務違反から生じる利益

本稿は、以下の順序に従って考察を進める。すなわち、原状回復法による保護を提案する見解の意義を明確にするために、まずアメリカ法における従前の個人情報漏えいの被害者保護の問題点について確認する(→Ⅱ)。次に、従前の個人情報漏えいの被害者保護のために原状回復法を用いる議論の低調な状況、その原因、およびその転換の契機を探ることとする(→Ⅲ)。その上で、近時の原状回復法による保護の動きとして、シヨルツとチャオの見解を若干詳しく紹介する(→ⅣおよびⅤ)。最後に、こうしたアメリカ法における議論、とりわけ、原状回復法による保護を志向する見解を整理し、その意義と問題点を指摘し、わが国の議論への示唆としたい(→Ⅵ)。

Ⅱ 従前の個人情報漏えいの被害者保護の問題点

(1) 概説

アメリカにおいては、個人情報の漏えいは、“data breach”と呼ばれている

の吐き出しにも目を向けるべきとする]も参照)。

第2に、個人情報を知的所有権と同様に扱い、それと同列の保護を与えることを試みる議論である。というのも、アメリカでは、知的所有権の侵害による救済手段として、利益吐き出しが広く認められており(ただし、特許権を除く)、個人情報を知的所有権として扱うことにより、そうした救済が認められる可能性が生じるからである。こうした可能性は、例えば、営業秘密と個人情報を対比的に論じ、前者の保護を後者にも及ぼそうとする見解において見られる(See, Lital Helman, *Trade Secrets and Personal Secrets*, 55 U. RICH. L. REV. 447 (2021))。

もっとも、両者の議論には、それぞれの問題がある。例えば、第1の議論に対しては、アメリカでも信認義務を認定することをめぐっては理解が分かれており(村上・前掲文献参照)、また(肯定する見解の中でも)信認義務の内容については論者でニュアンスが異なるとの指摘(村上・前掲39頁参照)も見られ、信認義務違反を説く見解すべてが利益吐き出しを認めるべきと提唱しているわけではない。また第2の議論に対して、秘密を守ることを目的とする点では両者は同一の系譜にあるものの、人格的性質を持つ個人情報を財産的性質の営業秘密と同列に扱うことには異論の余地があるであろう(プライバシーを知的所有権として扱う議論の問題点一般については, Samuelson, *Privacy As Intellectual Property?*, 52 STAN L. REV. 1126 (2000)を参照)。このような状況にあることに鑑みると、原状回復法それ自体により個人情報の漏えい被害者保護を志向する議論を検討することには一定の意味があると思われる。

が⁴²⁾、漏えいの被害者は、どの裁判所に対して、いかなる請求原因に基づき、訴えを提起することができるのであろうか。予めこの点について確認しておくことにしよう。

まず請求原因については、アメリカでは、個人情報の保護は、コモン・ロー、憲法、個人情報・プライバシー保護のための制定法（連邦法および州法）などの複数の法によってパッチワーク的な形で規律されており⁴³⁾、統一法の形では存在していない⁴⁴⁾。そのため、被害者は、自己に有利な請求原因を選択して請求することになる。例えば、コモン・ロー上の請求原因としては、過失による不法行為や契約違反などが用いられる。

次に、どの裁判所に請求するかについては、州法上の請求原因に基づき提起する場合には、州裁判所が管轄権を持つことになる。もっとも、クラスアクションが用いられた場合には、州裁判所とともに、連邦裁判所にも管轄権が認められる（連邦民事訴訟規則23条）。この場合には、両者の管轄権は競合することになり、どの裁判所に対して提訴するかは原告が訴訟戦略的な観点から決めることになるが⁴⁵⁾、近年の立法（2005年のクラスアクション公正法）による連邦裁判所の管轄の拡張に伴い、クラスアクションは連邦裁判所への移管が増えており、個人情報漏えい訴訟も連邦裁判所で扱われることが多い⁴⁶⁾。

そして連邦裁判所に提起する場合には、被害者は、合衆国憲法において要求

42) 佐藤・前掲注(15) 133頁。

43) アメリカの個人情報・プライバシー保護をめぐる法制度の状況については、さしあたり、西村あさひ法律事務所編・前掲書注(2) 622-649頁、松前恵環「米国個人情報・プライバシー保護法制をつかむ(第1回)米国の法制度の概要と近時の議論動向」NBL1185号(2021)79頁以下を参照。

44) ただし、近年、連邦レベルで包括的な統一法を制定しようとする動きもみられる。この点については、松前・前掲注(43)84頁以下、渡辺寛人「アメリカにおける連邦データプライバシー法案の動向」創価法学52巻1号(2022)33頁以下が詳しい。

45) 浅香吉幹「アメリカ弁護士のクラス・アクション戦略」東京大学法科大学院ロー・レビュー3号(2008)135頁、特に140頁以下を参照。

46) クラスアクションについては、溜箭将之『英米民事訴訟法』（東京大学出版会、2016）133頁以下を参照。また、情報漏えいとの関係については、松本慶「被告になる前に知っておくべき米国クラスアクション防御戦略（第9回）情報漏えい」ビジネスロー・ジャーナル11巻4号(2018)94頁以下を参照。

される「原告適格」が存在しなければならない（州裁判所に提起する場合はこの点は問題とならない）⁴⁷⁾。仮にこれを乗り越えたとしても、被害者は、各請求原因上の要件を充足することも必要となる⁴⁸⁾。

以下では、主として個人情報を管理する企業とそれを漏えいされた被害者との間に一定の契約関係がある中で個人情報漏えいが生じた場面を念頭に置いた上で、まず手続法上の問題として「原告適格」の問題について確認し、次に実体法上の問題として、コモン・ロー上の請求原因である不法行為に基づく請求と契約違反に基づく請求の障害を確認することとする⁴⁹⁾。これらの考察を通じて、全体として「損害」要件が個人情報漏えいの被害者にとって大きな障害となっていることが明らかになるであろう⁵⁰⁾。

(2) 手続法上の問題——憲法上の「原告適格」の障害

まず手続法上の問題として、連邦裁判所に提起する場合に問題となる「原告適格」要件について、その意義を確認した上で、その要件が個人情報漏えいの被害者保護との関係でもたらず障害について見ていくことにしよう。

47) See, Peter N. Salib & David K. Suska, *The Federal-State Standing Gap: How to Enforce Federal Law in Federal Court without Article III Standing*, 26 WM. & MARY BILL RTS. J. 1155, 1160 (2018)（「州裁判所は、合衆国憲法3編およびその原告適格の要件に服しない。」と指摘する）。

48) 以下で中心となる「損害」要件との関係で見ると、連邦裁判所に提訴する場合には、被害者は、原告適格のレベルにおける「損害」と各種の請求原因のレベルにおける「損害」の二つのレベルでの「損害」を立証しなければならないことになる (Solove & Citron, *supra* note 25, at 749)。

49) 本稿が取り上げる不法行為（特に過失によるそれ）と契約違反は、情報漏えい関連訴訟における請求原因として頻繁に用いられるものである（この点については、松本・前掲注（46）97頁の図表3を参照）。なお、コモン・ロー以外にも制定法上の請求原因として、頻繁に用いられるものもある（例えば、不公正な商慣習など）が、それらについては本稿では立ち入らない。

50) もっとも、アメリカにおける従来の個人情報漏えいの被害者保護の問題点については、既に複数の先行研究で指摘がなされている（例えば、佐藤・前掲注（15）135頁以下、佐々木・前掲注（15）、牛丸・前掲注（15）182頁以下など）。そのため、以下では、本稿の目的に必要な範囲で触れるにとどめる。

(i) 「原告適格」要件の意義

原告が、連邦裁判所において訴訟を遂行するためには、求めている救済を得るのに十分な個別的利益を有していることが求められる。この要件は、「原告適格(standing)」と呼ばれており、合衆国憲法3編第2条(Article III Section 2)に基づくものである⁵¹⁾。原告適格がない場合には、裁判所は、その訴訟の管轄権(jurisdiction)を有しないことになる。このような要件が要求される理由としては、裁判所の判決の結果を現実的に評価できるような具体的な事実的文脈の中で法的問題が提示されるよう確保する点に加えて、権力分立への配慮(原告適格要件なく行政の行為に裁判所が口出しすることは、大統領の執行権の侵害になるという点への配慮)という点も挙げられる⁵²⁾。

では、この原告適格は、どのような場合に認められるのであろうか。この点につき、判例は、具体的な要件としては以下の3点を挙げる⁵³⁾。すなわち、①原告が「事実として損害(injury in fact)」を被ったこと、②当該損害と争点となっている被告の行為の間で適正な因果関係を証明できること、③裁判所での勝訴判決によって救済されるものであることである。これらのうち、連邦最高裁判所は、原告適格の中心的な問題として①の要件を位置づけてきた⁵⁴⁾。そして、①の「事実としての損害」について、判例は「具体的かつ特定され(concrete and particularized)」かつ「推測的または仮定的ではなく、現実的または切迫している(actual or imminent)」ところの法律上保護された利益の侵害を被ったことを意味すると述べている⁵⁵⁾。このように連邦最高裁は、①の「損害」の理解についてかなり制限的な立場を採っているといえよう。そしてこのような

51) U.S. Const. art. III, § 2. 原告適格については、松井茂記『アメリカ憲法入門(第8版)』(有斐閣, 2018) 179頁以下、樋口範雄『アメリカ憲法』(弘文堂, 2017) 142頁以下を参照。

52) この点につき、松井・前掲書注(51) 192頁以下を参照。

53) *Lujan v. Defs of Wildlife*, 504 U.S. 555, 560-61 (1992).

54) *Danelle Keats Citron & Daniel J. Solove, Privacy Harms*, 102 B.U.L. REV. 793, 801 (2022).

55) *Friends of the Earth Inc. v. Laidaw Env't Serve. (TOC), Inc.*, 528 U.S. 168, 180 (2000).

「損害」の制限的な立場は、プライバシー侵害や個人情報漏えいの被害者の救済にとって大きな障害となる。次にこの点について見ていくことにしよう。

(ii) プライバシー侵害における「原告適格」の問題

連邦最高裁において個人情報漏えいの事案において原告適格の「損害」が直接争われた事案は見られないものの、個人情報漏えいケースに重大な影響を及ぼした⁵⁶⁾とされる *Clapper v. Amnesty Int'l USA* 事件⁵⁷⁾ は、プライバシー侵害の原告適格の「損害」について判断しているため、この点について確認しておくことにしよう。

本件は、疑わしきテロリストに対する監視を行う権限を拡大した外国情報監視法 (FIRA) の規定について、弁護士、ジャーナリスト、および活動家のグループが監視の合憲性について争った事案であった。原告は、自分達が NSA が疑わしいとみなす傾向がある外国人とコミュニケーションしているため、自分達のコミュニケーションが盗聴されていることを恐れていると主張した (なお、原告は、弁護士と依頼人の機密性を害する政府の監視を回避するための措置 [例えば、電話等を回避して、時間と費用をかけて直接依頼人の下を訪れるなど] も採っていた)。

これに対し、連邦最高裁判所は、(a) 監視についての恐れ (fear) および不安 (anxiety) ——そしてそれから防御するための措置を採る費用——は、推論的過ぎて、原告適格を正当化するための「事実としての損害」要件を満たすことができないと結論付けた⁵⁸⁾。もっとも、連邦最高裁は、同事件の判決の脚注において、(b) 「いくつかの例において」「損害が生じる『重大なリス

56) *Citron & Solove, supra* note 54, at 802.

57) 568 U.S. 398 (2013). 同事件の紹介としては、川澄真樹「アメリカ刑事法の調査研究 (148) *Clapper v. Amnesty International USA*, 568 U.S. __, 133 S.Ct. 1138 (2013)」比較法雑誌 50 巻 2 号 (2016) 408 頁以下、塚本宏達 = 遠本麻佑子「個人情報漏洩にかかる訴訟の原告適格——*Clapper* 判決および *Spokeo* 判決以降の連邦裁判所の裁判例に照らして」(2017) (https://www.noandt.com/wp-content/uploads/2017/10/us_no36.pdf) がある。

58) 568 U.S. 398, 422.

ク (substantial risk)』」が、原告に原告適格を付与するには十分になるとも述べている (ただし、何が重大なリスクに当たるかについては述べられていない) ⁵⁹⁾。

このような曖昧な判断に起因してか、ハッカーによる個人情報漏えいの事案などにおいて下級審の判断は分かれている ⁶⁰⁾。具体的には次の通りである。すなわち、多数の裁判例は、——Clapper事件の (a) の部分と同様に——個人情報漏えいの被害者に原告適格を否定する ⁶¹⁾。その根拠としては、①将来の損害リスクは、推論に過ぎず、確実に差し迫っていないこと、②将来の損害リスクから自らを防衛するための予防措置の費用により損害を認めることは、損害を「捏造する」ことを認めること、③個人情報漏えいが個人情報の主体にもたらす精神的苦痛は、個人情報が様々な方法で使用されるであろうとの推論に根拠づけられ、説得的でないことなどが挙げられる。これに対し、少数の裁判例は、——Clapper事件の (b) の部分と同様に——個人情報漏えいの被害者に原告適格を肯定する ⁶²⁾。その根拠としては、①ハッカーの攻撃による情報漏えいがある場合には、損害は仮定的ではなく、現実的であること (ハッカーは、そのような目的をもって、行っている) や②被害者が損害回避費用を被るのは合理的であることなどが挙げられる。

(iii) 小括

このように被害者が連邦裁判所に提訴する際には、「原告適格」の障害があり、そこでは「損害」要件が重要な要素となっており、個人情報漏えいの場面では認められる例がないわけではないものの、否定するものも多く、被害者の救済にとっては大きな障害となっているといえる ⁶³⁾。もっとも、これを乗り越えた

59) Solove & Citron, *supra* note 25, at 740 ; Citron & Solove, *supra* note 54, at 802.

60) Solove & Citron, *id.*, at 741-3. 以下の下級審の考察は、同論文に負う。

61) *E.g.* Reilly v. Cerdian Corp., 664 F.3d 38 (3d Cir. 2011).

62) *E.g.* Remijas v. Neiman Marcus Group, LLC, 794 F. 3d 688 (7th Cir. 2015).

63) なお、Clapper事件以後の連邦最高裁でプライバシー侵害において「損害」要件が争われた事案としては、Spokeo, Inc v. Robins, 136 S.Ct. 154 (2016) と TransUnion

としても、実体法上の要件との関係で障害ははまだ残る。そこで次にこの点について確認していく。

(3) 実体法上の問題①——不法行為に基づく請求の障害

ここでは、不法行為に基づく請求について見ていくことにしよう。アメリカにおける不法行為に基づく請求は、わが国のような一般的な規定ではなく、個別の類型毎に規律されているが、以下では、個人情報漏えいの場面において問題となり得るプライバシー不法行為に基づく請求と過失による不法行為 (negligence) に基づく請求について概観した上で⁶⁴⁾、各請求の障害について見ていくことにしよう。

(i) プライバシー不法行為に基づく請求とその障害

①概説

まず、プライバシーの不法行為に基づく請求について取り上げよう。古典的な理解によれば、プライバシー侵害に該当するのは、①私生活への侵入 (intrusion upon seclusion)、②名前や肖像の盗用 (appropriation of name or likeness)、③私的事柄の公開 (public disclosure of private facts)、④公衆への誤解 (false light) の4類型に該当する場合であるとされる。こうした理解は、周知のように、従前の判例法を体系化したプロッサーの類型論によるものであり⁶⁵⁾、その後、第2次不法行為リストイメントにおいても採用されてい

LLC v. Ramirez, 141 S. Ct. 2190 (2021) がある。

64) これら以外にも、不実表示 (詐欺や過失による不実表示など) に基づく不法行為請求も用いられる傾向があるとされる (Chao ①, *supra* note 37, at 564-5) が、個人情報漏えいの場面では用いにくいとされる。というのも、不実表示に基づく不法行為の重要な要素は、「信頼 (reliance)」の存在であるため、ここでの被害者が、不実表示に基づき請求するには、被害者がその不実表示を読み、そして信頼したことが要求されるが、多くの消費者は、プライバシーポリシーを読んでおらず、ましてそれらを信頼していないためである (Chris Jay Hoofnagle & Jennifer M. Urban, *Alan Westin's Privacy Homo Economicus*, 49 WAKE FOREST L. REV. 261, 304 (2014))。そのため、本稿ではこの点に立ち入らない。

65) William L. Prosser, *Privacy*, 48 CALIF. L. REV. 383 (1960) . なお、同論文について

る⁶⁶⁾。そして、多くの州において、このリステイトメントのプライバシー不法行為の規定が採用された⁶⁷⁾。そのため、個人情報漏えいの被害者は、これらのプライバシー侵害のタイプのいずれかに該当すると主張して、請求することになるであろう。

もっとも、プライバシー侵害に基づく請求には以下のような障害がある。

②障害1：「損害」要件

第1に、個人情報漏えいの被害者は「損害」を立証することができるかが問題となる。すなわち、プライバシーの不法行為についても「損害」要件の充足が求められる⁶⁸⁾。もっとも、裁判所は、従来、めったに損害の存在や多くのプライバシー不法行為を理由とする損害の根拠が純粋に精神的損害であるという事実に疑問を提起せず、損害の存在を当然の前提としてきた⁶⁹⁾。というのも、当初アメリカにおいてプライバシー侵害として問題となった事案が、マスメディアによる侵害であったからである⁷⁰⁾。

しかし、このような取扱いは、個人情報の収集、使用、そして開示を伴う現代のプライバシー問題においては同様に語ることはできない。というのも、先述のように、個人情報漏えいにおける損害は、——詐欺の被害など具体的な損害を被ることがない段階では——現実的なものとはいえないと解されているからである。そのため、このような「損害」要件の存在は、被害者の救済を阻止

は、石井夏生利『個人情報保護法の理念と現代的課題——プライバシー権の歴史と国際的視点』(勁草書房、2008) 150頁以下も参照。

66) RESTATEMENT (SECOND) OF TORTS § 652 (AM. L. INST. 1965).

67) Scholz ③, *supra* note 36, at 1652.

68) Citron & Solove, *supra* note 54, at 809 (不法行為法においてホームズが重視した「損害」要件について、プロッセラーも採用したと指摘する)。

69) *Id.* at 810.

70) これはいうまでもなく、プライバシーの生みの親であるサミュエル・ウォーレンとルイス・ブランダイスの論文 (Samuel D. Warrant & Louis D. Brandies, *The Right to Privacy*, 4 HARV. L. REV. 193 (1890)) において念頭に置かれていた事案である。サイトロンとソローは、それ以上の理由を述べていないが、おそらくは、マスメディアによるプライバシー侵害の場合には、被害の規模 (知られる人の人数) が大きかったことが影響しているのではないかと推測される。

してきたとされる⁷¹⁾。

もっとも、プライバシー侵害については、損害の証明が困難であるとして、名誉毀損と同様に「金銭的損失または物理的危害」の証明なしに、損害賠償を認められるとする理解も示されている⁷²⁾。そのため、このような理解を採用すれば、精神的苦痛にとどまる場合でも個人情報漏えいの被害者保護のための手段として用いる余地は残されているように見える。しかし、次の障害がある。

③障害2：「プライバシー侵害」の該当性

第2に、第1の前提としてそもそも個人情報の漏えいが、「プライバシー侵害」に該当するといえるかが問題となる。先述のプライバシー侵害の類型論は、もともと、プライバシーという主観的な権利が過剰に広がりすぎることを恐れて、当該権利を具体的な事実パターンに枠づけることを意図していた⁷³⁾。しかし、従来の類型は、今日のデータ駆動型社会における個人情報漏えいの問題を扱うには不十分であるとの指摘がなされている。というのも、プライバシー侵害の不法行為の類型は、通常、顧客の個人情報の喪失や不正使用に当てはまらない多様な要件（具体的には、プライバシー侵害の不法行為は、問題となっている情報が、「かなり不快であること」（類型①および③の場合）、情報が公に開示されること（類型③および④の場合）、あるいは顧客の名前や肖像が奪われること（類型②の場合）など）を要求するため、個人情報漏えいの被害者には利用しにくいためである⁷⁴⁾。

こうした問題が生じた背景には、プロッサーの提案が、プライバシー侵害の種類の固定化をもたらし、社会における新たなプライバシー侵害の事案に対応

71) Ryan Calo, *Privacy Harm Exceptionalism*, 12 COLO. TECH. LJ, 361, 361-2 (2014) (プライバシー侵害において損害を認定する際の裁判所の困難性を「プライバシー損害例外主義」と言及する)。

72) RESTATEMENT OF TORTS § 867 cmt. d (AM. L. INST. 1939). この点につき、佐々木・前掲注 (15) 99頁を参照。

73) Prosser, *supra* note 65, at 422-23. See also, Scholz ①, *supra* note 36, at 668.

74) Chao ①, *supra* note 37, at 564; Scholz ①, *id.* at 668.

できるような新しいプライバシー不法行為の創設を（少なくとも近年に至るまで）もたらさなかったという事情がある⁷⁵⁾。

そのため、個人情報漏えいを理由としてプライバシー不法行為に基づき請求するためには、収集段階ではなく、その後の利用段階にまで拡張した、新たなプライバシー侵害の類型論を構築することが必要となる⁷⁶⁾。こうした方向性は、データ主体に新たな権利を認めようとする近時のEUにおける立法⁷⁷⁾やアメリカの有力学説の提案⁷⁸⁾に現れているといえる。

④小括

このように、プライバシー不法行為には、「損害」要件と「プライバシー侵害」該当性の要件の障害があり、個人情報漏えいの被害者にとっては——少なくとも古典的なプライバシー侵害の類型を前提としたままでは——使いやすいものとはいえないであろう。

(ii) 過失による不法行為とその障害

①概説

次に、過失による不法行為に基づく請求について取り上げよう。個人情報漏

75) Citron & Solove, *supra* note 54, at 809.

76) Chao ②, *supra* note 37, at 8.

77) 具体的には、EUの一般データ保護規則（GDPR）に見られるような、①個人が自己の個人情報が収集されることに反対する権利（21条）、②第三者が個人のデータを有するとき、個人がデータにアクセスする権利（15条）、③他者により保有されている不正確なデータを修正する（訂正する）権利（16条）、④データを第三者により消去させる権利（「忘れられる権利」はその一種）（17条）などが挙げられる。これらの権利については、さしあたり、山本龍彦『おそろしいビッグデータ——超類型化AI社会のリスク』（朝日新聞、2017）169頁以下を参照。

78) 代表的なものとして、ビッグデータ時代におけるプロファイリングの問題にも留意した、ダニエル・ソロヴの見解——①情報収集、②情報処理、③情報拡散、④侵害の4類型に大別する——が挙げられる（Daniel J. Solove, *A Taxonomy of Privacy*, 154 U. PA. L. REV. 477, 483 (2006)）。なお、ソロヴの見解については、宮下紘『ビッグデータの支配とプライバシー危機』（集英社新書、2017）105頁以下、佃貴弘「アメリカにおけるPrivacy as Trust論の理論的前提——新たなプライバシー権論の構築に向けて」北陸大学紀要49号（2020）1頁、特に4頁以下を参照。

えいの被害者は、通常この請求原因を用いて請求するのが一般的であるとされる⁷⁹⁾。その理由としては、①企業の不十分なサイバーセキュリティ措置を採ったために、ハッカーが個人の個人情報へのアクセスができたことに加えて、②多くのケースにおいて、会社の行動を非合理的なものとして、あるいは産業基準を下回るものとして性格づけることができることが挙げられる⁸⁰⁾。

もっとも、このような請求をする際にも、被害者は以下のような「損害」要件の障害に直面することになる。

②障害1：経済的損失ルール

経済的損失ルールとの関係である。ここで、経済的損失ルールとは、物理的な損害や財産への損害がないと、純粹に経済的な損失をもたらす過失行為を理由とする不法行為は成立し得ないとする判例法理をいう⁸¹⁾。個人情報漏えいのケースにおいては、物理的な損害は滅多に生じないため、経済的損失ルールが適用されると、個人情報漏えいの被害者の請求は否定されることになる⁸²⁾。

従来、このような経済的損失ルールは、このルールが適用される当事者達の関係の違い（契約当事者が否か）によって異なる説明がなされてきた⁸³⁾。すなわち、①非契約当事者の場合には、上記ルールは、無制限の責任を防止するために機能すると解されるのに対し、②契約当事者の場合には、上記ルールは、当事者が契約を通じてリスクを配分することを促すためと解されてきた。個人情報漏えいの場面では、被害者は、①の場合もあれば、②の場合もあり、上記ルールが個人情報漏えいに適用されるか否か、そしてどのように適用されるか

79) Chao ①, *supra* note 37, at 565.

80) *Id.* at 565.

81) Catherine M. Sharkey, *Can Data Breach Claims Survive the Economic Loss Rule?*, 66 DEPAUL L. REV. 339, 341 (2017). なお、経済的損失ルールについては、さしあたり、木下毅「日米比較不法行為法序説 (2・完)」立教法学 29号 (1987) 51頁、特に 67頁を参照。

82) Chao ①, *supra* note 37, at 565.

83) Sharkey, *supra* note 69, at 344.

について混乱がある⁸⁴⁾。

ただし、上記ルールに対して、例外を認める州もある。例えば、原告に対する合理的な注意を伴って行動するために被告に特別の義務を課すことを正当化する特別の関係があるとき、経済的損失を理由とする過失による不法行為の請求を認める場合などである。そのため、どこに管轄が属するかで過失による不法行為の請求の結論が左右されることもあるとされる⁸⁵⁾。

もっとも、このような経済的損失ルールの例外が認められたとしても、もう一つの「損害」要件により被害者の請求は阻止されることもある。次にこの点について見ることにしよう。

③障害2：損害の認識可能性

第2に、損害の認識可能性との関係である。すなわち、個人情報漏えいの被害者は、認識可能な(cognizable)損害を証明しなければならない⁸⁶⁾。そのため、被害者は、様々な方法で「損害」を認識可能な形で被ったとして主張する。例えば、被害者は、将来の損害リスク(例えば、ID窃盗、詐欺、あるいは名誉毀損など)、自己の個人情報の経済的価値、彼らの個人情報盗まれる精神的苦しみ、そして彼らの情報の不正使用を回避するために予防措置を採る費用などの経済的損害を被ったという形である⁸⁷⁾。

しかしながら、裁判所は、被害者の上記主張のものを「損害」として認めない。というのも、①主張する損害が将来の損害のリスク、あるいは予防措置を採る費用であるとき、これらの損害が遠すぎ、または推論的すぎであり、②失われた個人情報不法行為法のもとで価値を有しないためである⁸⁸⁾。それゆえに、多くのプライバシー訴訟は、被害者の情報が現実的に不正に使用されてきたとき、実現性があるのみである(典型的には、ID窃盗およびクレジットカード

84) *Id.* at 344.

85) Chao ①, *supra* note 37, at 566.

86) *Ibid.*

87) Solove & Citron, *supra* note 25, at 749-50.

88) Chao ①, *supra* note 37, at 566.

詐欺の場合)。しかしながら、このような理解は、融通が利かず、技術の進歩が課す新しいタイプの損害に対応することを困難にすると指摘されている⁸⁹⁾。

④小括

このように、二つの「損害」要件の障害のために、過失による不法行為に基づく請求も個人情報漏えいの被害者の保護を困難にしているといえよう。

(4) 実体法上の問題②——契約違反に基づく請求の障害

最後に、被害者が契約違反に基づき請求する方法について概観した上で、その障害について見ていくことにしよう。

(i) 契約違反に基づく請求の概説

企業は、プライバシーポリシーの中で、一定のプライバシー約束を顧客に対してするのが一般的である⁹⁰⁾。具体的には、企業がどのように顧客データを使用し、また開示するかを制限する旨の約束（〔狭義の〕プライバシー約束⁹¹⁾、また企業が顧客データを守るために合理的な措置を採る旨の約束（セキュリティ約束⁹²⁾）である。しかし、現実には、杜撰な企業にとどまらず、多くの企

89) *Id.* at 567.

90) *Id.* at 559–61. See also, Allyson W. Haynes, *Online Privacy Policies: Contracting Away Control over Personal Information?*, 111 PENN ST. L. REV. 587, 593 (「2001年までに、最も人気な商業ウェブサイトの事実上すべてがプライバシー通知を有する」と指摘する)。

91) 具体的には、主要なアメリカの通信事業者は、プライバシーポリシーの中で加入者の位置情報等を第三者に売却しないとの規定が置かれているとされる (Chao ①, *supra* note 37, at 559)。ただし、修正する動きも見られる。例えば、AT & Tはこうした情報を販売することを2013年に発表した (この点につき、城田・前掲注 (40) 12頁参照)。

92) 例えば、General Motorsのプライバシーポリシーには、「我々は、あなたの情報を不当なアクセスや取得から保護するのに役立つために設計された合理的かつ十分な技術的、管理上の、そして物理的セキュリティおよび秘密性基準を維持する」との規定が設けられている (See, Chao ①, *id.* at 559)。

業が上記の二つの約束を破っているとされる⁹³⁾。このような場合には、顧客は、企業が上記の約束に違反したと主張して、契約違反に基づき損害賠償を請求する方法が考えられる。というのも、このようなプライバシーポリシーに対しても契約法の理論は原則として適用されると解されているからである⁹⁴⁾。

(ii) 障害

もっとも、このような契約違反に基づく請求にも、一定の障害がある。具体的な障害としては以下が挙げられる。

①障害1：契約としての拘束力

第1に、プライバシー約束は、いつもその企業と顧客の契約の一部を構成するとは限らないという問題がある。裁判所は、プライバシーポリシーを契約として承認することに消極的であるとの指摘がなされている⁹⁵⁾。その理由は、以下の点にある⁹⁶⁾。すなわち、訴訟において裁判所がプライバシー約束を実現するためには、その約束が顧客契約のどこかに組み込まれていることを要求する。組み込まれていない場合には、その企業は契約上の義務を負っているとはいえないため、契約違反とは評価されなくなる。つまり、企業と顧客との間にプライバシーポリシーが存在していたとしても、それが当然に法的拘束力を伴う契

93) Chao によれば、プライバシー約束を破る例としては、Facebook, Walmart, Google などの大企業におけるデータ共有の動きが、またセキュリティ約束を破る例として、枚挙に暇がないとされる (*Id.* at 560)。

94) Helman, *supra* note 41, at 457.

95) Citron & Solove, *supra* note 54, at 807. ただし、こうした理解に対しては、Omri Ben-Shahar & Lior Jacob Strahilevitz, *Contracting over Privacy: Introduction*, 45 J. LEGAL STUD. S1, at s7 (過去10年以上の判例の実証研究を通じて、多くの裁判所が現実には、プライバシーポリシーが消費者と会社との間の双務的な拘束力のある約束を含むと理解していることを示す) のように異論もあり、この点の学説の評価は(とりわけ消費者法研究者の間で)分かれているようである(See, Chao ①, *supra* note 37, at 562 n. 23; Scholz ①, *supra* note 36, at 670)。もっとも、本稿ではこの点には立ち入らない。

96) Chao ①, *id.* at 561-2. See also, Helman, *supra* note 41, at 457.

約になるとは限らないということである⁹⁷⁾。

②障害2：「損害」要件

第2に、仮にプライバシー約束を契約として拘束力があるものと捉えることができたとしても、「損害」要件が障害として存在する。そのため、被害者は、過失による不法行為の場面において「損害」の認識可能性要件を満たすために主張するのと同様に、多様な形で損害を被ったと主張する。

しかし、裁判所は、一般的に、そうした損害を理由として、被害者の請求を認めないとされる。その理由としては、——過失の不法行為法の場面における説明と重複する点もあるが——以下の点が挙げられる⁹⁸⁾。すなわち、①多数の裁判所は、個人情報漏えいにおけるID窃盗や詐欺のリスクを大部分推論的過ぎるとしてみていること、②裁判所は、統計化されていない個人情報が価値を有しないと考えていること、③少数の例外を除き、契約法は経済的損害のみを対象とし、非経済的損害を対象としておらず、その帰結として、個人情報漏えいの場面では、精神的苦しみ (emotional distress) による損害は、回復の対象とならないこと⁹⁹⁾が挙げられる。さらに、④裁判所は、一般的に将来の損

97) なお、プライバシーポリシーが契約として捉えられないとしても、プライバシーポリシーが約束手続の禁反言の法理に服することはある (Citron & Solove, *supra* note 54, at 807)。具体的には、契約が締結されることができ、あるいは締結されるべきであったが一定の理由のために、適切に締結されなかった文脈で、生じる傾向があるとされる (Scholz ①, *supra* note 36, at 670)。もっとも、その前提としてプライバシーポリシーへの「信頼」があることが必要とされている (この点につき、不実表示の不法行為と同様の側面がある。前掲注 (64) を参照) が、消費者は通常プライバシーポリシーを信頼していないため、これにより救済することは困難であるとされる (Chao ①, *supra* note 37, at 565)。

98) 以下の説明は、Chao ①, *supra* note 37, at 563 を参照。なお、チャオは、本文で挙げる理由の多く (とりわけ、①②④の理由) を Solove & Citron, *supra* note 25, at 750-53 に依拠している (ソロヴらの見解は、原告適格の「損害」要件との関係で論じるものであるが、チャオは、そこでの理解が、契約違反、不法行為や制定法上の請求においても妥当すると捉えている)。

99) Rudgayzer v. Yahoo! Inc., 2012 WL 5471148, at *6 (N.D. Cal. Nov. 9, 2012) (「現実の損害の証明なしの… [個人] 情報の単なる開示」は、契約違反の請求を支持するには「不十分である」と述べる)。

害から保護するための予防的措置をとったことを理由に個人に補償することに消極的であるという事情もある。すなわち、個人情報漏えいの被害者は、ID窃盗や詐欺のリスクを緩和するために、クレジット監視サービスに申し込むために時間や金銭などを費やすことがある。このような場合、被害者は、これらの費用が、個人データの不適切な開示で想定され得る特殊な金銭的価値を提示すると主張する。しかし、裁判所は、このような被害者の費用を損害の「捏造」として見るため、否定する。というのも、①の理由のように将来の損害リスクを拒絶するならば、将来の損害リスクを認識可能な金銭的な損失に変えるために現在において時間および金銭の支出を損害と捉えることはできないからである（そうしないと、結果的に、被害者を推論的な損害から保護することになる）¹⁰⁰⁾。

③障害3：因果関係

第3に、仮にプライバシーポリシーを契約として捉えることができ、かつ損害の問題をクリアすることができたとしても、個人情報漏えいの被害者にとっては、因果関係を立証することの障害がある¹⁰¹⁾。例えば、個人情報漏えいによる損害が、ID窃盗やクレジットカード詐欺によるものの場合、その損害を被告の具体的な侵害によるものであると立証することは困難となる。というのも、多くの会社が個人情報漏えいの被害を被っており、自己の損害が被告の企業からの漏えいによるものかを判断することは困難を伴うからである。

④小括

以上の障害があるため、個人情報漏えいの被害者にとっては、プライバシーポリシー違反を理由とする契約違反に基づく請求は有用な手法とはいえない¹⁰²⁾。この点につき、ある論者達の言葉を借りれば、「今日、契約法——形式

100) Chao ①, *supra* note 37, at 564.

101) *Id.* at 562.

102) *Id.* at 560.

的な契約と約束的禁反言——は、少なくともプライバシーポリシーを伴うウェブサイトに關しては、情報プライバシーの保護においてほとんど役割を果たさない。」¹⁰³⁾といえる。

(5) 従来状況の原因とそれに対する疑問

以上の考察からは、従来の議論においては、個人情報漏えいの被害者にとっては——細部を捨象すれば——プライバシーの「損害」が、しばしば、多くのコモン・ロー上の法理論のもとで認識可能な損害¹⁰⁴⁾、あるいは証明可能な損害¹⁰⁵⁾とは考えられていないために、大きな障害になっており¹⁰⁶⁾、被害者は、私的執行を通じて、自己の権利を実現することが困難になっていることが明らかになったといえよう¹⁰⁷⁾。

もっとも、こうした取扱いの原因としては、プライバシーの「損害」要件の性格に加えて、その他の事情もあるように思われる。ここでは、さしあたり以下の2点を指摘し、若干のコメントを加えておくことにしたい。

103) Daniel J. Solove & Woodrow Hartzog, *The FTC and The New Common Law of Privacy*, 114 COLUM. L. REV. 583, 596 (2014).

104) Chao ①, *supra* note 37, at 556.

105) Roberts, *supra* note 34, at para 1.

106) もっとも、アメリカでは、個人情報漏えいの事案については、数は必ずしも多いわけではないが、クラスアクションが用いられることもあり、その場合、企業は、クラス認証がされた後は、和解で決着するケースが多いため（この点につき、松本・前掲注(46)98頁以下を参照）、その限りではこうした「損害」要件の障害はないともいえるかもしれない。しかし、クラスアクションにおいて認められる損害賠償額は、その基礎をなす違法行為と不釣り合いであることが指摘されており、和解による賠償額も高額化していることを踏まえると、問題があろう。そのため、他のより穏やかな手段があるのであれば、それが望ましいともいえる。この点で、本稿が注目する原状回復法を用いる見解は、利益吐き出しをその候補として挙げている（*See*, Chao ①, *supra* note 37, at 581-2）。

107) なお、本稿で立ち入らなかった制定法による請求の場合においても、「損害」が要件として要求されているが（Calo, *supra* note 71, at 361）、裁判所は、精神的苦痛を損害として主張するだけでは不十分で、何らかの経済的損失等の具体的な損害の証明を要求しており、同様に「損害」要件が障害となっているとされる（佐々木・前掲注(15)109-110頁）。

(i) 個人情報漏えい問題に対する裁判所の無理解

第1に、裁判所が個人情報漏えいにより被害者に生じる損害について十分に理解していないという理解である。この点につき、アメリカの情報法研究者であるライアン・キャロは次のように述べている。すなわち、「裁判所および幾人の学者は、他の法領域と不釣り合いなプライバシーにおける損害の証明を要求する。多くの者も、直感に反して、その情報産業がどこか本当の外部性を生まない点で事実上すべてのその他の産業とは異なると仮定する。」¹⁰⁸⁾。このような理解によれば、外部性という点から見ると、個人情報漏えい問題も公害問題も同様に加害者に損害賠償責任を課すことにより解決されるべき事象とし捉えることができるが、実際上の被害の相違を踏まえると、両者を同列に語ることはできないこと、そしてその帰結として、個人情報漏えいの被害者は十分に救済されないことになるわけである。

しかし、このような理解に対しては、ビッグデータおよびAIの登場に伴う今日の情報駆動社会においては、個人情報の漏えいは、完全には阻止することは困難であるとしても、漏えいされた情報の利用が、その後の被害者の人生を左右することさえあり得る重大な事態であることを踏まえると¹⁰⁹⁾、未だ検討の余地があるように思われる。

(ii) 公的執行の問題として捉える理解

第2に、——第1の点を措くとしても——個人情報漏えいの問題は、私的執行ではなく行政機関による公的執行の役割であるとする理解である。すなわち、アメリカでは、個人情報の保護は、企業の自由な活動を尊重するために、個々の企業による自主規制に任せた上で、特定の分野につき、公的機関が監視するという仕組みが採られている¹¹⁰⁾。ここでの公的機関の担い手としては、連邦取

108) Calo, *supra* note 71, at 361.

109) ビッグデータ時代におけるプライバシーをめぐる問題については、さしあたり、山本・前掲書・注(77)を参照。

110) ここでの自主規制は、あくまでFTCという強力な法執行機関の権限やその監督を背景としたものであるとされる(松前恵環「米国個人情報・プライバシー保護

引委員会 (FTC: Federal Trade Commission)¹¹¹⁾ が重要である¹¹²⁾。すなわち、FTCは、FTC法5条で禁止される「不公正もしくは欺瞞的な行為または慣行」につき、消費者を保護するために、行政的措置と司法的措置を行う権限を有する。前者の例として、(和解条項に違反した場合の) 企業への高額な制裁金の賦課¹¹³⁾、また後者の例として、裁判所に予備的および終局的差止命令を求めること (なお、終局的差止命令に付随してエクイティ上の金銭救済の一種として利益吐き出しを請求することも認められていた¹¹⁴⁾) が挙げられる。このような強い権限がFTCに認められていることを踏まえると、個人情報漏えいの問題は、FTCに任せれば足り、被害者に私的な訴権を認める必要はないのではないかという疑問も出てくるであろう。

しかし、こうした理解に対しては、FTCの権限行使には恣意的な面があるとの指摘もあり¹¹⁵⁾、また、近時の判例は、FTCによる金銭救済の請求に消極的な立場を示したため¹¹⁶⁾、被害者自身に私的な訴権を認める必要性が完全にな

法制をつかむ (第12回・完) 日本の個人情報保護法制への示唆」NBL1207号 (2021) 74頁参照)。

111) FTCは、「合衆国のプライバシー規制システムの最大かつおそらく最も重要な構成要素」であるとされる (Solove & Hartzog, *supra* note 103, at 588)。なお、FTC一般については、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8号 (2014) E100頁以下、松前恵環「米国個人情報・プライバシー保護法制をつかむ (第9回) 米国における個人情報・プライバシー保護監督機関——FTCを中心に」NBL1201号 (2021) 85頁以下を参照。

112) FTCの他に、州の司法長官もプライバシー法を執行する際に重要な役割を担っているとの指摘も見られる (Daniel Keats Citron, *The Privacy Policymaking of State Attorneys General*, 92 NORTRE DAME L. REV. 747, 748-751 (2016)) が、ここでは立ち入らない。

113) Helman, *supra* note 41, at 459。また、牛丸・前掲注 (15) 213頁も参照。

114) 松前・前掲注 (111) 89頁参照。ただし、後述のように、近年、金銭救済を求める権限につき、判例変更が見られる。

115) Helman, *supra* note 41, at 474 (citing Gerard M. Stegmaier & Wendell Bartnick, *Psychics, Russian, Roulette and Data Security: The FTCs Hidden Data Security Requirements*, 20 GEO. MASON L. REV. 673, 689-94 (2013))。もっとも、FTCの法執行は法的に安定した態様で行われており、実務において、FTCの法執行例は先例として重視されていると指摘する見解もある (Solove & Hartzog, *supra* note 103, at 619-2)。後者につき、松前・前掲注 (111) 90頁も参照。

116) AMG Capital Mgmt., LLC v. FTC, 141 S. Ct. 1341, 1344, 1347-49 (2021)。この

いとまではいえないであろう。少なくともアメリカの近時の学説の動きは、そうした方向を示唆するように思われる。もっとも、その際には、私人にどのような訴権を認めるのがよいのかは別途検討を要する。というのも、これまで考察してきた損害賠償による訴権にも問題はあり、十分とはいえないからである。そこで登場するのが、原状回復法を用いることで保護を図ろうとする議論である。次に、こうした新たな動きについて見ていくこととするが、その前に、これまで議論のまとめをしていくことにしよう。

(6) 小括

これまでの考察からは以下の点が明らかになったといえる。

第1に、手続法上の問題として、連邦裁判所が管轄権を有する場合には、合衆国憲法の「原告適格」の要件があり、そこでは「事実としての損害」があることが重要な考慮要素となっており、個人情報漏えいの被害者にとって大きな障害となっていたことである。

第2に、個人情報漏えいの被害者が漏えいした企業に対して不法行為に基づき損害賠償請求する場合、大別すると、プライバシー不法行為に基づく場合と過失による不法行為に基づく場合があるが、いずれも問題があったということである。具体的には、前者については、①「損害」要件の問題、②（「損害」要件をクリアしたとしても）従来のプライバシー類型論を前提とすると個人情報漏えいがプライバシー侵害に該当するというためにはハードルが高いことが挙げられる。また後者についても①経済的損失ルールと②損害の認識可能性という2つの「損害」要件の障害が挙げられる。

第3に、個人情報漏えいの被害者が漏えいした企業に対して契約違反に基づき損害賠償請求するには、①プライバシー約束の契約としての拘束力の有無、②（拘束力があるとしても）「損害」要件の障害、③因果関係の障害があり、実際上用いることは困難であったということである。

点につき、松前・前掲注（111）89頁を参照。

第4に、上記3点を踏まえると、それぞれの場面に固有な問題もあるが、全体としては「損害」要件が個人情報漏えいの被害者の救済にとって大きな障害になっていること、そしてその原因は、①個人情報漏えいにより生じる「損害」について裁判所が理解していないことや②この問題が公的執行の問題であると考えられていることにあるが、いずれも異論の余地を含んでいるということである。

こうした議論を踏まえると、個人情報漏えいの場面においても、被害者は一定の訴権を有するべきであるように思われる。その際には、「損害」要件を乗り越えることを試みる議論は、本来のあるべき方向かもしれないが、以下では、それとは異なり、原状回復法を用いることでこのような状況を乗り越えようとする議論を取り上げることとしたい。

〔付記〕本稿は、科学研究費補助金（若手研究）（研究課題19K13552および22K13307）の成果の一部である。

