Vol.2022-EIP-96 No.17
2022/6/10

プライバシー侵害における損害

小向太郎[†1]

プライバシー侵害に対して損害賠償請求が認められるのは，日本でも米国でも，損害の発生がある場合に限られる．わが国の裁判では，本人の意思に反して個人情報が公開されれば，損害の発生があると認められる傾向にある．これに対して,事実上の具体的な損害が立証されなければ，米国では損害の発生が認められない．本報告は、プライバシー侵害訴訟における損害について、日本と米国の考え方を比較し，それぞれの課題について考察することを目的とする．

Harm of Privacy Invasion

TARO KOMUKAI[†1]

In both Japan and the USA, privacy invasion could be judicially liable only when the plaintiffs suffered harm. In Japanese courts, if personal information is disclosed against the person's will, courts basically recognize harm. In contrast, the harm would not be recognized in the US unless plaintiffs have suffered an “injury in fact”. The purpose of this paper is to compare and discuss the issue of harm in privacy invasion in Japan and the U.S.

1. プライバシー侵害に対する法的救済

1.1 日本におけるプライバシー侵害

日本では，プライバシー侵害に対して，不法行為として損害賠償が請求できると考えられている．

民法第 709 条は，「故意又は過失によって他人の権利又は法律上保護される利益を侵害した者は、これによって生じた損害を賠償する責任を負う」と定めており，この条文から，不法行為の成立要件は，(1) 加害者の故意または過失，(2) 他人の権利利益侵害・違法性，(3) 加害者の責任能力，(4) 損害の発生，であると考えられている．つまり，損害の発生が，要件の一つとなっている[1]．

そして，「他人の身体、自由若しくは名誉を侵害した場合又は他人の財産権を侵害した場合のいずれであるかを問わず、前条の規定により損害賠償の責任を負う者は、財産以外の損害に対しても」賠償が認められている（民法第 710 条）．

プライバシー侵害に対する損害賠償に関して司法判断を示したものとして，「宴のあと」事件に対する 1964 年の第 1 審判決がある．この判決では，「私人がその私生活について他人から干渉されず，私的なできごとについてその承諾なしに公表されることから保護される」としてプライバシー侵害による不法行為の成立を認め，その成立要件として「公開された内容が（イ）私生活上の事実又は私生活上の事実らしく受けとめられるおそれのある事柄であり，（ロ）一般人の感受性を基準にして当該私人の立場に立った場合公開を欲しないであろうと認められること，（ハ）一般の人々に未だ知られていない事柄であること」を提示している[2]．その後の裁判例でもこの考え方が踏襲されている．

つまり，このような「公開を欲しないであろうと認められる」情報の公開は，それ自体が損害であると考えられてきたといって良い．

1.2 損害の認定

当初,「公開を欲しないであろうと認められる」情報は，当事者間だけの秘め事や前科のような，本人が秘匿することが社会の共通認識となっているものであると理解されていた．しかし，個人情報の利用が広がるとともに,「公開を欲しない」と認められる情報の範囲は，広くなる傾向にある．

早稲田大学江沢民主席講演会名簿提出事件では，学籍番号，住所，氏名，電話番号など「個人識別のための単純な情報」も「法的保護の対象で無断開示は違法」と位置づけ，「承諾を求めることが困難だった事情はうかがえないのに同意の手続きを取っておらず，情報の適切な管理についての期待を裏切った開示はプライバシーの侵害で不法行為となる」と判示している[3]．これ以降，本人の意思に

†1 中央大学
Chuo University

反する個人情報の開示については，広く不法行為の成立を認められており，これが損害の発生に当たるのかどうかについては，あまり問題とされていない．

1.3 情報漏えいと損害

本人の「公開を欲しない」という期待を保護するという考え方は、いわゆる情報漏えい事案でも採用されている。

ベネッセの顧客情報が流出した事件では，大阪高裁が，「プライバシーの侵害による上告人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」ことを理由に請求を棄却した事例がある[4]．

しかし，最高裁は，早稲田大学江沢民主席講演会名簿提出事件を引用して，「氏名，性別，生年月日，郵便番号，住所及び電話番号並びに B の保護者としての上告人の氏名といった上告人に係る個人情報」は，「上告人のプライバシーに係る情報として法的保護の対象となるというべき」であり，本件の漏えいによって侵害が生じているとして，大阪高裁に差し戻している[5]．大阪高裁は，差戻し審では損害の発生を認めている[6]．

このように，わが国のプライバシー侵害では，個人情報が本人の意思に反して公開されること自体が，不法行為の要件である損害に当たるという考え方が一般的になっていると言って良い．

2. 米国におけるプライバシー侵害

2.1 不法行為の成立要件

米国では，いわゆるプロッサーの 4 類型[7]にあたる，(1) 他人の干渉を受けずにおくっている隔離された私生活への侵入，(2) 他人に知られたくない事実の公表，(3) 一般の人に誤った印象を与えるような事実の公表，(4) 営利目的での氏名や肖像などの不正利用，について，不法行為責任が認められるとされている．また，米国には，データ侵害を受けた情報の本人に，私的訴権を認める立法が数多くあり，それに基づいて訴訟が提起されることがある．

これらの訴訟において，合衆国憲法第 3 条に基づき原告が訴訟を起こす資格（原告適格）を有するには，損害の発生が必要であると考えられている．損害がなければ，そもそもこうした責任を追求するための訴訟を提起する原告適格が認められないとして却下される[8]．

原告適格が認められるために，原告は，事実上の損害を主張しなければならず，その損害は，具体的かつ特定的で、「思い込みや仮定のものではなく、実際または差し迫ったもの」でなければならないとされている[9]．

また，訴因が認められずに請求が棄却される可能性もある．

プライバシー侵害に関しては，プロッサーの 4 類型にあてはまる典型的なケースでは，裁判所は損害の存在を推定する傾向にある．しかし，個人情報の収集，使用，開示に関わる現代的プライバシーが問題となる事例については，損害の認定がされない事が多い[10，p. 755]．

2.2 損害の認定

米国では，データの漏えいや不正利用などのデータ侵害に関する訴訟の多くが，連邦裁判所に提訴されるか，連邦集団訴訟公正化法（CAFA）に基づき州裁判所から移送されるa．集団訴訟では，原告と被告で異なる州に居住している者がいて，500 万ドルを超える州法上の請求がなされる場合には，連邦裁判所に移送されるからである．連邦裁判所が採用している基準では，原告適格を満たすために，事実上の損害を主張する必要があり，次にそれぞれの主張における訴因の要素を満たすために損害を主張立証しなければならない．Solove=Criton の研究によると，原告がこうした訴訟で主張している損害は，次の 3 つに大別することができる[11]．

(1) データ侵害が将来の損害のリスクを生じさせる（将来の損害リスク）
(2) 原告が損害のリスクを低減するために予防措置をとる必要に迫られる（予防コストの損害）
(3) データ侵害によって個人情報が漏洩した結果、原告が不安を経験する（不安の損害）

まず，「(1) 将来の損害リスク」については，ほとんどの場合，認識可能な損害として認められない．単にデータが漏洩しただけでは，データを入手した者の動機は不明であり，ID 窃盗やその他の金融詐欺による「事実上の損害」が発生していない．こうした被害はすぐに発生するものではないため，被害のリスクが「確実に差し迫っている」ことを証明するのは困難である．ハッカーが個人データに

a ClassActionFairnessActof2005,28U.S.C.§1332(d)(2012).

アクセスしており，その悪意ある動機が推察されるようなケースでも，裁判所は被害を認めていないb.

「(2) 予防コストの損害」に関しては，情報漏えいによって生じうる将来の損害のリスクを事前に予防するために，時間やコストを費やすことが損害だという主張がされている．将来のリスクをより認識しやすい金銭的損失に変えて主張するものだといえるが，こうしたものを「事実上の損害」と認めることについても，裁判所は否定的である[11, p. 753]．

「(3) 不安の損害」についても，裁判所は，ほとんどの場合，個人情報の盗取や悪用リスクの増加による原告の 恐怖，不安，精神的苦痛は，損害であると認めるには足りないと考えている[12]．

つまり，被害が直感的で，目に見えるもので，定量的に測定可能なものであることを求めているのであり，物理的，金銭的，または財産的損害があるか，少なくとも差し迫っていなければ損害が認められないのである[11, p. 754])．

このような米国の状況について，Solove=Criton は，裁判所が極端に消極的な態度を取っていることを批判し，リスクや不安を適切に評価することで，データ侵害における損害を認めることができるという提言をしている．

2.3 救済が行われた例

米国では，厳格で，経済的な損害がかなりはっきりと認められる場合でないと損害賠償責任が認められない傾向がある，一方で，経済的損失が認められるうる場合には，集団訴訟の提起や高額な和解金による解決がなされている．

情報漏えいに対して和解金が支払われた事例としては，大手小売店であるターゲットの事例がよく知られている．ターゲットは，2013 年にサイバー攻撃を受けて 4,100 万人の消費者に関するデータが流出したと言われている．流出したデータは，氏名，電話番号，電子メールアドレス，支払いカード番号，クレジットカード認証コード，その他の機密データであるとされる．本件については各州政府が調査を行っていたが，2017 年 5 月にターゲットが，1850 万ドルを支払うことで和解したと報じられている[13]．

本件は，情報の内容から，経済的な被害が発生する蓋然性も高く，訴訟の長期化によって企業イメージが既存される恐れがあることなどが，高額の和解に至った背景にあると考えられる．

3. 考察

3.1 日米の比較

以上のように，プライバシー侵害による損害の発生について，日米では大きな考え方の違いがある．

米国では，損害の発生について具体的な損害を厳格に求めており，経済的な損害がかなりはっきりと認められる場合でないと損害賠償責任が認められない傾向がある．一方で，経済的損失が認められるうる場合には，集団訴訟の提起や高額な和解金による解決がなされている．日本では，このような高額な補償が行われた事例だけが注目される傾向がある．しかし，基本的に日本で認められているような，漠然とした不安を損害として認めて損害賠償責任が認められることは，米国ではない．

一方で，日本のプライバシー侵害に対する不法行為責任は、損害の発生を要件としているが、本人の期待権の侵害という比較的緩やかな考え方が採用されており，損害の発生は広く認められる．そして，過失についても，漏えいという結果が生じていれば比較的広く認められる傾向にある．ただし，認められる損害賠償額は比較的少額である．

米国において，裁判所が不法行為責任等を認めるにあたって「損害」を厳格に求めてきた背景には，濫訴の危険性が、日本に比べて大きいということがあると考えられる．日本でも，消費者集団訴訟制度の導入時などに濫訴を懸念する声があったが，現在のところ大きな問題になっていない[14]．制度自体の課題も指摘されているが，司法文化の違いや，法曹人口の違いも大きい．

3.2 補償と抑止効果

不法行為に対して損害賠償責任等を負わせることの本来の目的は，「①被害者の権利の価値を回復させる（金銭による権利の価値を実現する）ことによる保護と，②行為者（加害者）の行動自由の保障である」とされる[15]．

このうち，①は，その損害を塡補して損害がなかったのと同じ状態にすることであり，後者は過失責任主義によって過失がない行為を行う権利を補償することであると考えられている．

しかし，日本の情報漏えい事案等で取られている損害の発生を広く認め，少額の賠償を認める考え方は，損害を補填するよりも，このような結果に至

b Solove=Critron（2018）752 頁では，このような裁判所の判断例として，Forbes v. Wells Fargo Bank, 420 F. Supp. 2d 1018, 1019, 1021 (D. Minn. 2006) などをあげている．

った者に法的な責任を負わせるという規範的な価値判断に基づくものだと言える．つまり，このような考え方の背景には，同種の行為が今後起きないように注意を換気するという抑止効果への配慮があると考えられる．

3.3 情報漏えいに関する制度

情報漏えいに関して，情報管理者に対して何らかの法的責任を負わせる制度としては，(1) 民事的責任（損害賠償），(2)安全管理措置義務，(3)データ侵害通知義務，がある[16]．わが国において，(1) 民事責任（損害賠償）について，広くその責任を認める傾向にあることはすでに述べたとおりである．(2) 安全管理措置義務については，個人情報取扱事業者に対する安全管理措置義務が課せられており，(3) データ侵害通知義務についても，2020 年の改正で漏えい等があった際に個人情報保護委員会への報告や本人への通知等が義務付けられている．

これら各制度がおかれている趣旨は，本来は，(1) 民事責任（損害賠償）が被害者の損害に対する補填を目指すものであり，(2)安全管理措置義務と(3)データ侵害通知義務が，情報セキュリティ対策の向上とずさんな管理の抑止を目指すものであるといえる．

4. おわりに

日本の情報漏えい事案における損害賠償請求訴訟では，被害者が被った損害の補償を確保するとともに，このような結果に至った事業者等に対して法的責任を認めることによる社会的な制裁を課し，同種の問題が生じないようにする抑止効果も期待して，判断がくだされていると考えられる．

しかし，損害賠償請求の本来の目的は，被害者に生じた損害の補填である．情報セキュリティ対策を向上させ，そのような被害が起こらないようにするための制度が，これとは別に整備されているのであれば，ある程度の制度的な棲み分けを行うべきである．また，たまたま漏えいを生じた事業者に対して広く法的責任を認めて，社会的な制裁を加えるような考え方では，情報セキュリティ対策が促進される効果はあまり期待できない．

このような棲み分けの必要性は，情報セキュリティ対策の向上を目指す 2 つの制度（安全管理措置義務とデータ侵害通知義務）についてもいえる．例えば，データ侵害通知は，運用によっては漏えいを起こした企業等を安全管理措置義務違反であるとして公表し，その企業の社会的信用を毀損することで制裁を課すという性格を持ちうる．しかし，データ侵害通知制度の本来の目的は，データの漏えいも含めてリスクの状況の透明性を高め，より公的な対策を行うことにある．データ侵害通知の制度を制裁的な意味合いをもって運用すれば，重大なデータ侵害の事実の隠蔽を助長してしまう可能性もある．むしろ，有効な情報共有を促すような制度の運用をすべきである．

情報の収集蓄積が飛躍的に増大するなかで，情報セキュリティ向上の社会的課題としてさらに重要になることは疑いがない．しかし，データの漏えいを始めとするデータ侵害を完全に根絶することは不可能である．どうすれば情報管理者の情報セキュリティ対策の動機を高めて，有効な情報セキュリティ対策を促すような制度や運用を実現していくことが重要である．

謝辞

本研究は，科学研究費補助金・基盤研究(C)(課題番号: 18K01393)による研究費を得て実施した．

参考文献

[1] 小向太郎『情報法入門』(NTT 出版，第 6 版，2022) 176 頁.
[2] 東京地判昭 39・9・28 下民集 15 巻 9 号 2317 頁.
[3] 最二小判平 15 年 9 月 12 日民集 57 巻 8 号 973 頁.
[4] 大阪高判平 28 年 6 月 29 日判タ 1442 号 48 頁.
[5] 最二小判平 29 年 10 月 23 日判タ 1442 号 46 頁.
[6] 大阪高判令元年 11 月 20 日判時 2448 号 28 頁.
[7] William L. Prosser, Privacy, 48 Cal. L. Rev. 383 (1960).
[8] Lujan v. Defenders of Wildlife, 504 U.S. 555,560 (1992).
[9] Friends of the Earth Inc. v. Laidlaw Envtl. Servs. (TOC), Inc., 528 U.S. 167,180 (2000).
[10] Danielle Keats Citron and Daniel J. Solove, Privacy Harms, 102 Boston Univ. L. Rev. 793 (2022).
[11] Daniel J. Solove and Danielle Keats Citron, Risk and Anxiety: A Theory of Data Breach Harms, 96 Texas L. Rev. 737 (2018),750.
[12] Amburgy v. Express Scripts, Inc., 671 F.Supp.2d 1046, 1053 (E.D.Mo.2009).
[13] USA Today, Target to pay $18.5M for 2013 data breach that affected 41 million consumers, May 23, 2017.
[14] 日本経済新聞「使われぬ消費者集団訴訟」2021 年 11 月 21 日.
[15] 潮見佳男『不法行為法 I』(信山社，第 2 版，2009) 13 頁.
[16] Daniel Solove and Woodrow Hartzog, BREACHED! WHY DATA SECURITY LAW FAILS AND HOW TO IMPROVE IT (2022).