

MIGA コラム「新・世界診断」

「個人情報流出と損害賠償責任」のその後

佐藤智晶

武蔵野大学国際総合研究所客員准教授

青山学院大学法学部准教授

東京大学公共政策大学院特任准教授



医療分野に関する法政策が専門で、関連領域として信託法制を研究。2008 年にワシントン大学ロー・スクール

(LL.M.)、2010 年に東京大学博士 (法学)。2009 年 4 月から 8 月にかけて東京大学大学院法学政治学研究科特任研究員、2009 年 9 月から東京大学で勤務し、2015 年 4 月からは青山学院大学法学部に准教授として着任。2012 年 8 月からは 2016 年まで、ブルッキングス研究所経済部局医療政策部門客員研究員も歴任。著書として『アメリカ製造物責任法』(弘文堂・2011 年)、主要論文は PLOS Medicine 等に掲載。

個人情報等のデータの流出は、関係者にとって頭の痛い問題である。流出させた側は、会社のレピュテーションや株価への悪影響、被害者は悪用への懸念に悩まされることになる。

もっとも、現実を直視すれば、われわれは日々、個人情報を誰かに渡して生活しており、本人は個人情報が流出された認識がないにもかかわらず、日々大量のスパムメールが届く人も少なくない。

個人情報の流出が半ば日常化している中で、時には大企業が個人情報を流出させてしまうニュースが報じられることもあり、その被害者の数は数十万人、数百万人にのぼり得る。

このような場合に、どのような法的解決が図られるべきかは、現代社会が抱える困難な問題の一つであるといえる。

本コラムでは、以前執筆した拙稿(「個人情報の流出と損害賠償責任: 欧米の事例を参考に」判例時報 2336 号(2017 年) 133-141 頁、以下「拙稿」。)の執筆後の展開を追いかけて、個人情報の流出と損害賠償責任についていまだ残されている問題点を指摘したい。刊行後の日本の裁判例として筆者が把握しているものは、東京地判平成 30 年 6 月 20 日(判例①、賠償責任を否定)、千葉地判平成 30 年 6 月 20 日、判例時報 2399 号 46 頁; 判例タイムズ 1459 号 186 頁; 金融・商事判例 1564 号 38 頁(賠償責任を否定)、東京地判平成 30 年 12 月 27 日、判例タイムズ 1460 号 209 頁; 1564 号 38 頁(判例②、B 社のグループ会社 S に、1 人当たり 3,300 円、計約 150 万円の支払いを命じた。B 社の責任は否定)、東京高判令和 1 年 6 月 27 日(B 社と同社のグループ会社 S に、1 人当たり 2,000 円の支払いを命じた)、などである。

拙稿でも述べたとおり、筆者は、わが国において個人情報

報の流出につき一定の範囲で慰謝料が認められるべきだという見解を非難するつもりはない。拙稿で分析した事例（実損がない限り慰謝料をゼロとする傾向にある）は基本的にあくまで米国におけるものであり、日本法の下においては日本特有の議論がありうることはいうまでもないからである。

ただ、他方で、冒頭述べたとおり、我が国においても個人情報の流出が日常化しているうえ、対象者の数が多いために流出した側が倒産しかねないほど慰謝料の額が巨額になり得る。このような実情に照らすと、単に個人情報が流出したにとどまり、実損が発生していない被害者について、慰謝料の金額をどの程度とすべきかは、非常に悩ましい問題である。

現在、このような実損が未だ発生していないケースにおいて、流出それ自体をもって慰謝料が発生し得るのか、発生するとして慰謝料の額をどう定めるべきかについて確立された実務慣行は存在しない。

そして、裁判例においても前述のとおり結論が分かれている。すなわち、Yahoo! BB 事件では、1 人につき 6,000 円（5000 円の慰謝料と 1000 円の弁護士費用）、判例①では、「B 社側がおわびの文書と 500 円相当の金券を配布したことなども考慮し、・・・慰謝料が発生するほどの精神的苦痛があるとは認められない」¹とされたのに対し、判例②では、個人情報流出した可能性を認めつつ、現時点においてダイレクトメール等が増えた気がするという程度以上に財産的損害その他の実害が原告らに生じたこととはうかがわれないとしながらも、1 人あたり慰謝料として 3,000 円、弁護士費用として 300 円の計 3300 円の損害賠償責任を認めている。

以上のように確立された判例や実務慣行の未だ存在しない我が国の現状に鑑みれば、米国等における実務上の方向性は今後の我が国の実務のあるべき姿を検討するうえで参考になるものと考えられる。

この点に関連して、筆者は、多数人の個人情報が流出し、流出情報の悪用が未だ確認されていない事案において、慰謝料（損害賠償）を認めている日本以外の国の裁判例をいまだ発見できていない。米国の事例にとどまらず、他国の事例もできる限りリサーチしているにもかかわらず、である。日本では、1 人当たり 2,000 円、あるいはもっとも認めるべきだという議論が行われていることとは対照的である²。

念のため言及しておくが、海外において、慰謝料が認められているように見える事案もないわけではない。しかしながら、これらには看過できないほどの実損が生じている、あるいは極めて秘匿性の高い個人情報が流出したという特殊性がある。

まず、英国の TLT v Secretary of State for the Home Department.[2016] EWHC 2217 (QB) は、精神的苦痛の損害賠償を認めている³。

しかしながら、この事案はきわめて特殊である。なぜなら個人情報は亡命者のものであり、政府による情報流出によって身の安全に危険を覚え、しかも転居等を余儀なくされたからである。情報流出によって身体

¹ 「ベネッセへの損賠請求認めず、14 年発覚の情報流出巡り東京地裁判決」 日本経済新聞（2018 年 6 月 21 日）朝刊 40 頁。

² こうした金額では、被害者側にとっては救済とはいえない範囲にとどまるのに対し、流出側は債務超過になるほどの出捐を強いられることもあり得るのであり、実質的に見ても実効性に乏しい。

³ Robin Hopkins, New High Court judgment on privacy and data protection damages, Panopticon, Oct. 10, 2016, available at <https://panopticonblog.com/2016/10/10/new-high-court-judgment-privacy-data-protection-damages/>

に対する具体的な危険が発生し、しかも実費（転居費用）まで発生している事例と、一般的な情報流出の事案を同一には扱うことはできないように思われる。ちなみに、認められた賠償額は、1 万 2,500 ポンド、2,500 ポンド、3,000 ポンド、6,000 ポンド、3,000 ポンドというように、原告ごとに大きく異なっている。

次に、英国の WM Morrison Supermarkets Plc v Various Claimants [2018] EWCA Civ 2339 では、ある企業の従業員が同僚の個人情報を含むデータ（10 万人分）を故意にファイル転送サービスサイトにアップロードし、実際に当該データにアクセスがあった事件で、企業が約 5,000 人の従業員から使用者責任等を問われている事案で⁴、第一審と高裁では使用者責任の成立が認められている（最高裁が上告を受理しているが、結論は出ていない）⁵。もっとも、当該事案においては、被害者の氏名、住所、性別、生年月日、電話番号（自宅と携帯）のみならず、公的医療保険の保険証番号、銀行支店番号、銀行口座番号に加え、企業から支払われていた給与額という極めて秘匿性の高い個人情報までがファイル転送サービスのウェブサイト上にアップロードされ、誰もが閲覧可能な状態におかれ、実際にアクセスがあったという特殊性がある⁶。

先に述べた慰謝料の流出側に与える過度のダメージに加え、このような海外の実情をも考慮すると、今後、我が国において個人情報の流出に慰謝料を認めていくことになったとしても、個人情報が流出したというだけで慰謝料を認めることには慎重であるべきと考える。すなわち、慰謝料を認めるか否か、認めるとしてその金額をどの程度とすべきかは、いかなる個人情報が流出したのか、個人情報の流出に際して被害者が具体的にいかなる対応を余儀なくされたか（引越し、クレジットカードの再発行など）などの具体的事情を考慮して決せられるべきであり、特段の実損はないが気分を害したという程度で慰謝料を認めることは、適切とはいえないと考える。

付言するに、われわれはどうしても被害者の側、すなわち、個人情報等のデータを流出させられる場面ばかりを想像するが、われわれは加害者にもなり得るという視点も忘れてはならない。現代社会では、皆が個人情報等のデータを委ね合っており、常に流出させるリスクに同様にさらされているからである。

たとえばある者が携帯電話を紛失し、あるいは盗まれた場面を想像してみると、それを返してもらえな

⁴ 争点は、"the question whether an employer is liable, directly or vicariously, for the criminal actions of a rogue employee in disclosing personal information of co-employees on the web, whether under the Data Protection Act 1998, an action for breach of confidence, or in an action for misuse of private information"である。

⁵ Ben Sigler, Court of Appeal hands down significant judgment in WM Morrison Supermarkets Plc ("Morrisons") v Various Claimants [2018] EWCA Civ 2339, Stephenson Harwood LLP, Oct. 25, 2018, available at [http://www.shlegal.com/news/court-of-appeal-hands-down-significant-judgment-in-wm-morrison-supermarkets-plc-\(-morrison-s\)-v-various-claimants-2018-ewca-civ-2339](http://www.shlegal.com/news/court-of-appeal-hands-down-significant-judgment-in-wm-morrison-supermarkets-plc-(-morrison-s)-v-various-claimants-2018-ewca-civ-2339); Herbert Smith Freehills LLP, Latest twist in the Morrisons Case: Supreme Court grants Morrisons permission to appeal, Apr. 23, 2019, <https://hsfnotes.com/data/2019/04/23/latest-twist-in-the-morrison-s-case-supreme-court-grants-morrison-s-permission-to-appeal/>

⁶ この事件では、責任のみが争われており、損害額については争点となっていない点に留意されたい。故意による情報流出行為が、使用者責任の成立を左右する雇用の範囲内の行為かどうか大きな争点である。See Various Claimants v Wm Morrisons Supermarket PLC [2017] EWHC 3113 (QB) 2017, para 10.

れば個人情報を含んだディスクが他人の手に渡ったのと同じことであり、個人情報が流出したと言い得るが、仮に流出の事実をもって慰謝料請求が認容される可能性が高くなると、携帯電話の所有者は情報の登録されていた大勢の者らに対し慰謝料を支払わなければならない可能性がある（そして、単なる流出だけで実害がなくとも賠償されるというのであれば、携帯電話でなくとも、eight などの名刺管理会社や facebook をはじめとする SNS サービスに本人に無断で職場情報やメールアドレス、携帯電話番号を登録しただけでも、本人に断りなく第三者に流出させたとして慰謝料請求が認められるということになりかねない。）。このようなケースで考えてみれば、少なくとも、その流出された個人情報が何者かに利用され、電話がかかってくるなどの実害が発生していないにもかかわらず、慰謝料請求を認容することが適切とはいいがたいことが理解されよう。

かかる考え方に対しては、企業と個人は異なるのであり、企業は巨額の賠償リスクを負わない限り、個人情報の管理を行うインセンティブに欠けるという反論があるかもしれない。

しかし、我が国の損害賠償制度は再発予防や懲罰の目的で金額を定めるものとはなっていない。モラルハザードのリスクに対しては、個人情報保護法において課徴金の定めを置くなどの他の方法によって立法的な解決が可能であろう。

最後に、拙稿の刊行後の新たな情報について若干のアップデートをしておきたい。

まず、カリフォルニア州では、消費者プライバシー保護法が可決成立した⁷（まだ施行されていない（2020 年 1 月 1 日施行予定））。同法によれば、制定法上の損害額が一事案ごと、一カルフォルニア州民あたり 100 ドルから 750 ドルないし実損のうち大きな額、として規定されており、金額は比較的大きいといえる。他方で、要件として、①対象となっている個人情報は暗号化されていない、または匿名化されていないものとされ、②流出の対象は社会保障番号、運転免許証番号ないし州民 ID 番号、銀行口座番号、セキュリティコード付きのクレジットないしデビットカード番号、医療情報、医療保険情報のみとされており⁸、③当該個人情報が不正アクセス、流出、盗難、または開示された場合に限定され、④被告が情報の特性に適した合理的なセキュリティ手順および慣行を導入および維持する業としての義務に違反した場合などとされており、適用範囲がかなり限定されている。

同法の要件に該当しない場合の損害賠償を排斥する趣旨か否かを含め、その法解釈、損害の考え方、損害

⁷たとえば、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 年）91-126 頁、121 頁以下で紹介されている。同論文では、当事者適格を満たすための損害、不法行為法ないし制定法上の損害賠償責任の要件としての損害、さらには損害額の算定の問題が扱われている。ほかには、渋谷江里子「個人情報保護、米でも新法、カリフォルニア州、欧州に続き、企業の準備期間短く」日本経済新聞（2019 年 5 月 27 日）朝刊 11 頁を参照のこと。

⁸ CAL. CIV. CODE § 1798.150(a) and 1798.81.5 (d). See Sullivan & Cromwell LLP, California Consumer Privacy Act of 2018, July 2, 2018, at 6-7, available at <https://www.sullcrom.com/files/upload/SC-Publication-New-Statute-Introduces-Privacy-Protections-for-California-Consumers-and-Subjects-Businesses-to-Potential-Liability.pdf>

の算定方法⁹などは明らかとなっておらず¹⁰、今後の実務の蓄積が待たれるところであるが、我が国の実務上の運用を考える際の参考となり得る。

次に、アメリカで 2014 年に発生した、サイバー攻撃によって約 1,000 万人の**社会保障番号と個人識別可能な医療情報**が健康保険組織（Premera Blue Cross）から漏洩した事案については、連邦裁判所に集団訴訟が提起されていたが、ようやく和解案がまとまった（オレゴン地区連邦地方裁判所の承認待ちの状況）¹¹。当該和解案では、7,400 万ドルの和解額のうち、4,200 万ドルが 3 年間のデータセキュリティ改善関連のために、3,200 万ドルが被害者救済関連のために充てられる予定となっている（内訳には、クレジットカードの不正利用監視費用（350 万ドルまで）、弁護士費用（1,400 万ドル）、被害者への金銭的な補償（1,000 万ドル）などが含まれる）。被害者への金銭的な補償（1,000 万ドル）の具体的な内容について言えば、実損の填補は 1 人あたり 1 万ドルまで、個人情報の流出対応によって喪失した時給等への填補は 1 人あたり 400 ドルまでになっており、実損の証明を一切必要としない救済額は原則 1 人あたり 50 ドル（カリフォルニア州居住者については、“California Confidentiality of Medical Information Act, CMIA”という州制定法に基づ

⁹ 制定法上の損害額の算定方法について、同法律では、裁判所は、不正行為の性質と重大性、違反の数、不正行為の永続性、不正行為が発生した期間、不正行為をした被告の害意、被告の資産、負債、および純資産等のうち、当事者のいずれかが訴訟において提示した 1 つ以上の関連するものを考慮しなければならない、と規定されている。CAL. CIV. CODE §§ 1798.150(a)(2).

¹⁰ See, e.g., Kristen J. Mathews and Courtney M. Bowman, The California Consumer Privacy Act of 2018, Privacy Law Blog by Proskauer Rose LLP, July 13, 2018, available at <https://privacylaw.proskauer.com/2018/07/articles/data-privacy-laws/the-california-consumer-privacy-act-of-2018/>; Sullivan & Cromwell LLP, California Consumer Privacy Act of 2018, July 2, 2018, available at <https://www.sullcrom.com/files/upload/SC-Publication-New-Statute-Introduces-Privacy-Protections-for-California-Consumers-and-Subjects-Businesses-to-Potential-Liability.pdf>

¹¹ See Gene Johnson, Premera Blue Cross pays states \$10 million over data breach, Washington Post, July 11, 2019, available at https://www.washingtonpost.com/business/technology/premera-blue-cross-pays-states-10-million-over-data-breach/2019/07/11/70264650-a407-11e9-a767-d7ab84aef3e9_story.html?utm_term=.5c4f158440c5; Linn F. Freedman, Premera Blue Cross Settles for \$10M with 30 States for 2014 Data Breach, July 18, 2019, available at <https://www.natlawreview.com/article/premera-blue-cross-settles-10m-30-states-2014-data-breach>; Kaiser Health News, 30 States Sign \$10.4M Agreement With Premera Blue Cross Over Data Breach Impacting Millions, July 12, 2019, available at <https://khn.org/morning-breakout/30-states-sign-10-4-million-agreement-with-premera-blue-cross-over-data-breach-impacting-millions/> See also Plaintiff's First Amended Consolidated Class Action Allegation Complaint on In re Premera Blue Cross Customer Data Security Breach Litigation, No. 3:15-md-2633-SI (D. Ore. filed on Sep. 30, 2016), available at <https://www.tousley.com/uploads/pdf/premerafirstamendedcomplaint.pdf>; In re Premera Blue Cross Customer Data Security Breach Litigation, No. 3:15-md-2633-SI (D. Ore. Feb. 9, 2017); Unopposed Motion for Preliminary Approval of Proposed Settlement Agreement on In re Premera Blue Cross Customer Data Security Breach Litigation, No. 3:15-md-2633-SI, slip op. at 7-13 and 59-61 (D. Ore. filed on May 30, 2019), available at <https://www.tousley.com/uploads/pdf/unopposedmotionforpreliminaryapproval.pdf>

いて追加的に 50 ドル) を受け取ることができる可能性がある。もっとも、3,200 万ドルのうち被害者への金銭的補償の総額としては 1,000 万ドルが予定されているに過ぎないため、仮に被害者全員が実損の証明を一切必要としない救済を申請した場合、1 人あたりの支払いは、およそ 1 ドルになってしまう。社会保障番号と個人識別可能な医療情報が実際に漏洩した場合でさえ、このような救済となっている点は、最新の実務として参考になるだろう。また、情報を漏洩してしまった保険者は、30 の州から別訴を提起され、和解のために約 1,000 万ドルを支払うことになった。こちらは、被害者の救済のためのものではないが、額の算定の観点からはおよそ被害者 1 人あたり 1 ドル、という計算になる¹²。

¹² See Plaintiff's First Amended Consolidated Class Action Allegation Complaint on In re Premera Blue Cross Customer Data Security Breach Litigation, No. 3:15-md-2633-SI (D. Ore. filed on Sep. 30, 2016), available at <https://www.tousley.com/uploads/pdf/premerafirstamendedcomplaint.pdf>; In re Premera Blue Cross Customer Data Security Breach Litigation, No. 3:15-md-2633-SI (D. Ore. Feb. 9, 2017); Unopposed Motion for Preliminary Approval of Proposed Settlement Agreement on In re Premera Blue Cross Customer Data Security Breach Litigation, No. 3:15-md-2633-SI, slip op. at 7-13 and 59-61 (D. Ore. filed on May 30, 2019), available at <https://www.tousley.com/uploads/pdf/unopposedmotionforpreliminaryapproval.pdf>