GDPR における企業・団体の法的責任

亜細亜大学法学部　加藤隆之

1　民事責任（82 条）

（1）GDPR

要件

①規則違反行為

②因果関係

③有形的又は無形的損害（material and non-material damage）（tangible and intangible damages）

→・EU データ保護指令 23 条では、単に「損害」を被った者が損害賠償を請求できるとなっている。損害の種類は明示されていない。

名誉権侵害に基づく損害（reputational injury）を含む。

財産的損害を伴わない純粋な精神的な損害、例えば、不安や懸念（apprehension）、また、不快感（discomfort）などを含むかが問題[1]。

・GDPR33、34 条では、個人データの侵害行為があった場合、監督機関やデータ主体にその事実を通知する義務が存在するが、自然人の権利又は自由に対するリスクが生じそうにない場合にはその義務が免除されている。この risk 概念との整合性も問題。

（2）日本の状況

(a) 個人情報保護法違反と損害賠償請求

日本では、個人情報保護法違反、プライバシー権侵害があった場合、不法行為による損害賠償請求（民法 709 条）という法律構成が一般的である。

①個人情報保護法違反＝709 条の違法性あり？、権利侵害あり？

②権利侵害≠損害　この点は明らか。

③損害＝精神的損害を含む？

(b) 早稲田大学講演会事件

早稲田大学が、中国主席の講演会に参加予定の学生の情報（学籍番号、氏名、住所、電話番号）を防犯を理由にその提供を求めた警視庁に応じたという事件（最判平成 15・9・12）。

①プライバシー権侵害？　→　最高裁は、「秘匿されるべき必要性が必ずしも高いものではないが、自己が欲しない他者にはみだりにこれを開示されないという期待は保護されるべきであり、本件個人情報は、プライバシーにかかる情報として法的保護の対象となる」とし、「本件開示について承諾を求めることは容易であった」ことなどを理由として、プライバシー権の侵害であると判示した（ただし、第 1 審、2 審は不法行為の成立を否定し、最高裁も 3 対 2 の僅差での判決）。

⇓

個人情報であることは間違いない（ただし、当時個人情報保護法は成立していない）。しかし、個人情報＝プライバシー権？、情

[1] 個人情報保護違反があった場合、アメリカ契約法において「損害」要件を認定することの困難性を指摘する論稿として、平野晋「情報プライバシー侵害に対する米国契約法の限界」別冊 NBL 情報通信法制の論点分析（商事法務、2015 年）を参照。「損害」概念そのものは、契約法理と不法行為法理とで異ならないことに鑑みると、同様の問題が後者でも生じるはずである。

報開示＝プライバシー権侵害？？反対に、プライバシー権にかからない個人情報とは何か？

②損害はあり？　→　何の損害？

③損害額の算定として正しい？　→　１人当たり 5,000 円（差戻審で認定）は正当？
ベネッセの顧客情報（子、保護者の氏名、住所、電話番号、性別、生年月日）流失は？500 円は少なすぎる？3000 万人×500 円＝150 億円？

Cf.　長崎市内の公立小学校において、通知表の様式及び評定記載方法めぐる校長会と教師との争いから、一部の学校では通知表が児童に交付されないという出来事が起きたため、Y がこの教師たちを批判したビラを配布し、そこに彼らの氏名・年齢・住所・電話番号を記載していたという事件（最判平成元年 12 月 21 日）。
→最高裁は、当該個人情報の頒布行為によって、私生活の平穏など人格的利益が侵害されたことを理由として、2 万円の損害賠償を認めた。

２　制裁金（83 条）

（１）制裁金対象団体

(a) 民間団体

(b) 公的団体については、各国の裁量事項（7 項参照）
→公的団体に対して制裁金を科したとしても、その金銭の出所は結局のところ税金であり、その実効性に乏しいという批判があるため。

（２）制裁金を科す際の考慮事項

制裁金は、監督機関の是正措置と共に科すことも可能であるが、次の事項を考慮して制裁金を科すか否かについて決定しなければならない（2 項）。

(a) 当該取扱いの性質及び目的並びに影響を受けたデータ主体の数及びデータ主体の受けた損害の程度を勘案した当該違反行為の性質、重大性及び期間。
(b) 当該違反行為の故意又は過失の特徴。
(c) データ主体の受ける損害を軽減させるために当該管理者及び取扱者がとった行動。
(d) 第 25 条及び第 32 条に従って管理者及び取扱者が実施した技術的及び組織的対策を勘案した当該管理者及び取扱者の責任の程度。
(e) 当該管理者又は取扱者による関連する以前の違反行為。
(f) 当該違反行為の是正及び違反により生じ得る悪影響軽減のためになす監督機関との協力の程度。
(g) 当該違反行為によって影響を受ける個人データの種類。
(h) 当該違反行為が監督機関へ知らされた方法。特に管理者又は取扱者が当該違反行為を通知したか否か、もし通知したのならその範囲。
(i) 同じ事項に関して、当該管理者又は取扱者に対して事前に第 58 条第 2 項で定められた措置が命じられていた場合、それら措置の遵守。
(j) 第 40 条によって承認された行動規範又は第 42 条による承認された認証メカニズムの遵守。
(k) 当該違反行為から直接又は間接を問わず得られた財政上の利益又は避けられた損失のように、当該事案の状況に該当する悪化又は軽減要素。

↓

確かに、こうしたことを考慮するべきではあろうが、いかんせん、次の制裁金対象の違反行為が広汎すぎる。

（３）制裁金対象の違反行為

(a) 1,000 万ユーロ又は全世界年間売上高 2 パーセント以下の制裁金（4 項）
①管理者及び取扱者による次の条文の義務違反行為

・8 条　情報社会サービスに関する子どもの同意に対して適用される条件
（Conditions applicable to child's consent in relation to information society services）
・11 条　識別を要求しない取扱い（Processing which does not require identification）
・25 条　データ保護・バイ・デザイン及びバイ・デフォルト
（Data protection by design and by default）
・26 条　共同管理者（Joint controllers）
・27 条　EU 域内に拠点のない管理者又は取扱者の代理人
（Representatives of controllers or processors not established in the Union）
・28 条　取扱者（Processor）
・29 条　管理者又は取扱者の権限下における取扱い
（Processing under the authority of the controller or processor）
・30 条　取扱い活動の記録（Records of processing activities）
・31 条　監督機関との協力（Cooperation with the supervisory authority）
・32 条　取扱いのセキュリティ（Security of processing）
・33 条　個人データ侵害の監督機関への通知
（Notification of a personal data breach to the supervisory authority）
・34 条　データ主体への個人データ侵害の通知
（Communication of a personal data breach to the data subject）
・35 条　データ保護影響評価（Data protection impact assessment）
・36 条　事前協議（Prior consultation）
・37 条　データ保護職の指名（Designation of the data protection officer）
・38 条　データ保護職の地位（Position of the data protection officer）
・39 条　データ保護職の職務（Tasks of the data protection officer）
・42 条　認証（Certification）
・43 条　認証機関（Certification bodies）

②認証機関による次の条文の義務違反行為
・42 条　認証（Certification）
・43 条　認証機関（Certification bodies）

③監視団体による次の条文の義務違反行為
・41 条 4 項　承認された行動規範違反に対するの監視団体の適切な措置
（41 条、Monitoring of approved codes of conduct）

（b）2,000 万ユーロ又は全世界年間売上高 4 パーセント以下の制裁金（5、6 項）
次の条文の違反行為
・5、6、7、9 条における、同意の条件を含む基本的取扱い原則
・12～22 条におけるデータ主体の権利
・44～49 条に従った第三国又は国際機関の取得者への個人データ移転
・9 章に基づき採択された加盟国の国内法の義務
・取扱いに関する 58 条 2 項による監督機関の命令の不遵守、又は 58 条 1 項に違反してアクセスの提供を履行しないこと

↓

3 大特徴　＝　広汎性、曖昧性、高額性
・広汎性、曖昧性としては、たとえば、17 条（忘れられない権利）、31 条、33 条、36 条を参照。

・2016年のグーグル年間売上高（予想）は、８兆円規模なので、そのうちの4%となると最高200億円までの制裁金を科すことも可能となる。200万ユーロ（24億円）どころではない！！
・さらに、損害賠償責任と刑事責任すら負う？？他の権利とバランスを失していないだろうか？
・理論上は、小規模の事業者に対しても、高額な制裁金を科すことも可能。
・制裁金を科さない加盟国とアンバランスではないだろうか？

（4）制裁金を科さない制度の採用

83条9項では、制裁金を科す制度を採用していない場合、（条文の文言はfineとしかないが、刑事罰である罰金を指す？）制度で代替することを認めている。

→たとえば、アイルランドでは、制裁金をデータ保護コミッショナーが科すことについて、憲法上の制約があり（34.1，37.1）、現在でも同コミッショナーは制裁金を科す権限はない。

3　刑事責任（84条）

特に83条による制裁金を欠く場合には、罰則が必要？

→・制裁金を欠く場合とは相当狭くないだろうか？
　・83条による制裁金が科される場合には、これで足りる？

4　まとめ

①民事責任　→　損害概念のとらえ方いかんでは、責任を負うべき範囲が、非常に広汎になる可能性あり。
②制裁金　→　対象行為が広汎に過ぎる　＋　高額に過ぎる
③刑事罰　→　各国で一貫性なし

↓

EU域内に拠点を持ち、EEA域外にEU市民の個人データを移転するなどGDPRの適用を受ける企業は、責任を負担する場合の予見が立てにくいため、過剰な対策をせざるを得ない傾向にあるのではないだろうか。
確かに、高額な制裁金を科される可能性もゼロではない。しかし、リスクを強調しすぎることもフェアな見解ではない。

↓

ところで、そもそも、こうした事態はなぜ生じるのか。

↓

・個人情報保護法違反の行為態様が多様である。
　→このことはやむを得ないとしても、少なくとも、GDPRの制裁金対象行為は広すぎる。
・プライバシー権と個人情報保護との関係が不明確すぎる。
　→個人情報保護をプライバシー権と同様の人権であると位置づけるのは妥当か？
・なぜプライバシー権が重要で、最も保護される領域は何かについての原理的考察が希薄。
　→英米の判例法は、パッチワークでプライバシー権を十分に保障しないといわれているが、そこに意味はまったくないのか。
・個人情報保護については、より一層、原理的考察が希薄。
　→こうした基礎理論の研究をおろそかにしたままで、個人情報保護を声高に主張して、その実効性確保のみを強調する、いわば原理主義的主張がまかり通ってはいないだろうか。

（もっとも、これまで、新しい個人情報保護という分野における法規制を作り上げるために精一杯であったという事情があるようにも思われる。）

↓

その結果、いかなる個人情報保護違反行為に対し、民事制裁、刑事制裁、行政上の制裁金制裁が妥当なのかを決する「価値基準」を失っている。

（参考資料）

関連条文（加藤訳）

第82条　賠償請求権及び法的責任
Article 82 Right to compensation and liability

1. 本規則の違反行為によって有形的又は無形的損害を受けた者は、管理者又は取扱者からその受けた損害に対する賠償を受ける権利を有するものとする。

1. Any person who has suffered material or non-material damage as a result of an infringement of this Regulation shall have the right to receive compensation from the controller or processor for the damage suffered.

2. 取扱いに関与する管理者は、本規則に違反する取扱いによって生じた損害に対して責任を負うものとする。取扱者は、取扱者に対して明示的に向けられた本規則の義務を遵守しない場合、又は管理者の適法な指示の範囲を超えた若しくはこの指示に反する行動をとった場合に限り、取扱いによって生じた損害に対して責任を負う。

2. Any controller involved in processing shall be liable for the damage caused by processing which infringes this Regulation. A processor shall be liable for the damage caused by processing only where it has not complied with obligations of this Regulation specifically directed to processors or where it has acted outside or contrary to lawful instructions of the controller.

3. 管理者又は取扱者は、損害を生じさせた事実に対して何ら責めに帰すべき事由がないことを証明した場合、第2項に基づく法的責任を免除されるものとする。

3. A controller or processor shall be exempt from liability under paragraph 2 if it proves that it is not in any way responsible for the event giving rise to the damage.

4. 複数の管理者若しくは取扱者又は管理者及び取扱者が同じ取扱いに関与しており、第2項及び第3項に基づいて、取扱いによって生じたあらゆる損害に対して責任を有する場合、各管理者又は取扱者は、データ主体に対する実効的な賠償を確保するため、全損害に対して責任を負うものとする。

4. Where more than one controller or processor, or both a controller and a processor, are involved in the same processing and where they are, under paragraphs 2 and 3, responsible for any damage caused by processing, each controller or processor shall be held liable for the entire damage in order to ensure effective compensation of the data subject.

5. 管理者又は取扱者が、第4項に従い、受けた損害に対する賠償の全額を支払った場合、当該管理者又は取扱者は、同じ取扱いに関与した他の管理者又は取扱者から、第2項で規定された要件に従い、彼らの責任部分に相当する賠償額を求償する権利を有するものとする。

5. Where a controller or processor has, in accordance with paragraph 4, paid full compensation for the damage suffered, that controller or processor shall be entitled to claim back from the other controllers or processors involved in the same processing that part of the compensation corresponding to their part of responsibility for the damage, in accordance with the conditions set out in paragraph 2.

6. 賠償請求権の行使に関する裁判手続は、第79条第2項で定める加盟国の国内法に基づく管轄裁判所に提起されるものとする。

6. Court proceedings for exercising the right to receive compensation shall be brought before the courts competent under the law of the Member State referred to in Article 79(2).

第83条　制裁金の一般条件
Article 83 General conditions for imposing administrative fines

1. 各監督機関は、第4項、第5項及び第6項で定める本規則の違反に関して、本条に従った制裁金の賦課が、個々の事案において、実効的、比例的なものであり、かつ抑止的効果を有するよう確保しなければならない。

1. Each supervisory authority shall ensure that the imposition of administrative fines pursuant to this Article in respect of infringements of this Regulation referred to in paragraphs 4, 5 and 6 shall in each individual case be effective, proportionate and dissuasive.

2. 制裁金は、個々の事案の状況により、第58条第2項(a)号から(h)号及び(j)号で定める措置に加え、又はこれに代えて科されるものとする。個々の事案において、制裁金を科すか否かについて、また、制裁金の額について決定するにあたっては、次に掲げる事項を考慮しなければならない。

2. Administrative fines shall, depending on the circumstances of each individual case, be imposed in addition to, or instead of, measures referred to in points (a) to (h) and (j) of Article 58(2). When deciding whether to impose an administrative fine and deciding on the amount of the administrative fine in each individual case due regard shall be given to the following:

(a) 当該取扱いの性質及び目的並びに影響を受けたデータ主体の数及びデータ主体の受けた損害の程度を勘案した当該違反行為の性質、重大性及び期間。

(a) the nature, gravity and duration of the infringement taking into account the nature scope or purpose of the processing concerned as well as the number of data subjects affected and the level of damage suffered by them;

(b) 当該違反行為の故意又は過失の特徴。

(b) the intentional or negligent character of the infringement;

(c) データ主体の受けた損害を軽減させるために当該管理者及び取扱者がとった行動。

(c) any action taken by the controller or processor to mitigate the damage suffered by data subjects;

(d) 第25条及び第32条に従って管理者及び取扱者が実施した技術的及び組織的対策を勘案した当該管理者及び取扱者の責任の程度。

(d) the degree of responsibility of the controller or processor taking into account technical and organisational measures implemented by them pursuant to Articles 25 and 32;

(e) 当該管理者又は取扱者による関連する以前の違反行為。

(e) any relevant previous infringements by the controller or processor;

(f) 当該違反行為の是正及び違反により生じ得る悪影響軽減のためになした監督機関との協力の程度。

(f) the degree of cooperation with the supervisory authority, in order to remedy the infringement and mitigate the possible adverse effects of the infringement;

(g) 当該違反行為によって影響を受ける個人データの種類。
(g) the categories of personal data affected by the infringement;

(h) 当該違反行為が監督機関へ知らされた方法。特に管理者又は取扱者が当該違反行為を通知したか否か、もし通知したのならその範囲。
(h) the manner in which the infringement became known to the supervisory authority, in particular whether, and if so to what extent, the controller or processor notified the infringement;

(i) 同じ事項に関して、当該管理者又は取扱者に対して事前に第 58 条第 2 項で定められた措置が命じられていた場合、それら措置の遵守。
(i) in case measures referred to in Article 58(2) have previously been ordered against the controller or processor concerned with regard to the same subject-matter, compliance with those measures;

(j) 第 40 条によって承認された行動規範又は第 42 条による承認された認証メカニズムの遵守。
(j) adherence to approved codes of conduct pursuant to Article 40 or approved certification mechanisms pursuant to Article 42; and

(k) 当該違反行為から直接又は間接を問わず得られた財政上の利益又は避けられた損失のように、当該事案の状況に該当する悪化又は軽減要素。
(k) any other aggravating or mitigatingfactor applicable to the circumstances of the case, such as financial benefits gained, or losses avoided, directly or indirectly, from the infringement.

3. 管理者又は取扱者が故意に又は過失で、同じ又は連鎖した取扱い作業に関して、本規則の複数の規定に違反した場合、制裁金の総額は重大な違反に対して定められた額を超えてはならない。
3. If a controller or processor intentionally or negligently, for the same or linked processing operations, infringes several provisions of this Regulation, the total amount of the administrative fine shall not exceed the amount specified for the gravest infringement.

4. 次に掲げる規定の違反行為に対しては、第 2 項に従って、1,000 万ユーロ、又は事業である場合、前会計年度の全世界年間売上高の 2%のいずれか高額な方を限度として、制裁金を科すものとする。
4. Infringments of the following provisions shall, in acccordance with paragraph 2, be subject to administrative fines up to 10 000 000 EUR, or in the case of an undertaking, up to 2 % of the total worldwide annual turnover of the preceding financial year, whichever is higher:

(a) 第 8 条、第 11 条、第 25 条、第 26 条、第 27 条、第 28 条、第 29 条、第 30 条、第 31 条、第 32 条、第 33 条、第 34 条、第 35 条、第 36 条、第 37 条、第 38 条、第 39 条、第 42 条及び第 43 条における管理者及び取扱者の義務。
(a) the obligations of the controller and the processor pursuant to Articles 8, 11, 25, 26, 27, 28, 29, 30, 31, 32, 33, 34, 35, 36, 37, 38, 39, 42 and 43;

(b) 第 42 条及び第 43 条における認証機関の義務。
(b) the obligations of the certification body pursuant to Articles 42 and 43;

(c) 第 41 条第 4 項における監視団体の義務。
(c) the obligations of the monitoring body pursuant to Article 41(4).

5. 次に掲げる規定の違反行為に対しては、第 2 項に従って、2,000 万ユーロ、又は事業である場合、前会計年度の全世界年間売上高の 4%のいずれか高額な方を限度として、制裁金として科すものとする。
5. Infringements of the following provisions shall, in accordance with paragraph 2, be subject to administrative fines up to 20 000 000 EUR, or in the case of an undertaking, up to 4 % of the total worldwide annual turnover of the preceding financial year, whichever is higher:

(a) 第 5 条、第 6 条、第 7 条及び第 9 条における、同意の条件を含む基本的取扱い原則。
(a) the basic principles for processing, including conditions for consent, pursuant to Articles 5, 6, 7 and 9;

(b) 第 12 条から第 22 条におけるデータ主体の権利。
(b) the data subjects' rights pursuant to Articles 12 to 22;

(c) 第 44 条から第 49 条に従った第三国又は国際機関の取得者への個人データ移転。
(c) the transfers of personal data to a recipient in a third country or an international organisation pursuant to Articles 44 to 49;

(d) 第 9 章に基づき採択された加盟国の国内法の義務。
(d) any obligations pursuant to Member State law adopted unter Chapter IX;

(e) 第 58 条第 2 項に従った監督機関による取扱いに関する一時的若しくは一定期間の制限若しくは命令、若しくはデータ流通の一時停止に従わないこと、又は第 58 条第 1 項に違反してアクセスの提供を履行しないこと。
(e) non-compliance with an order or a temporary or definitive limitation on processing or the suspension of data flows by the supervisory authority pursuant to Article 58(2) or failure to provide access in violation of Article 58(1).

6. 第 58 条第 2 項で定める監督機関による命令の不遵守に対しては、本条第 2 項に従い、2,000 万ユーロ、又は事業である場合、前会計年度の全世界年間売上高の 4%のいずれか高額な方を限度として、制裁金を科すものとする。
6. Non-compliance with an order by the supervisory authority as referred to in Article 58(2) shall, in acccordance with paragraph 2 of this Article, be subject to administrative fines up to 20 000 000 EUR, or in the case of an undertaking, up to 4 % of the total worldwide annual turnover of the preceding financial year, whichever is higher.

7. 第 58 条第 2 項による監督機関の是正権限を妨げることなく、各加盟国は、当該加盟国に設置された公的機関若しくは団体に制裁金を科すか否か、また、いかなる程度制裁金を科すかについて定めることができる。
7. Without prejudice to the corrective powers of supervisory authorities pursuant to Article 58(2), each Member State may lay down the rules on whether and to what extent administrative fines may be imposed on public authorities and bodies established in that Member State.

8. 本条に基づく監督機関による権限の行使は、EU 法及び加盟国の国内法に従った実効的な司法的救済及び適正手続を含めた適切な手続的保護措置に従うものとする。

8. The exercise by the supervisory authority of its powers under this Article shall be subject to appropriate procedural safeguards in accordance with Union and Member State law, including effective judicial remedy and due process.

9. 加盟国の法体系が制裁金の定めを欠く場合、本条は、管轄監督機関によって主導されかつ管轄国内裁判所によって科される罰金という形で適用される。この場合、加盟国の法体系は、それらの法的手段が実効的であり、監督機関によって科される制裁金と同等の効果をもつよう確保するものとする。いかなる場合でも、科される罰金は、実効的、比例的なものであり、かつ抑止的効果を有するものでなければならない。当該加盟国は、2018 年 5 月 25 日までに本項に従って加盟国が採用する国内法の規定、及び、その後の改正法又はそれらの規定に影響を及ぼす改正についても、遅滞なく、欧州委員会に通知しなければならない。

9. Where the legal system of the Member State does not provide for administrative fines, this Article may be applied in such a manner that the fine is initiated by the competent supervisory authority and imposed by competent national courts, while ensuring that those legal remedies are effective and have an equivalent effect to the administrative fines imposed by supervisory authorities. In any event, the fines imposed shall be effective, proportionate and dissuasive. Those Member States shall notify to the Commission the provisions of their laws which they adopt pursuant to this paragraph by 25 May 2018 and, without delay, any subsequent amendment law or amendment affecting them.

第 84 条　罰則
Article 84 Penalties

1. 加盟国は、本規則違反、特に第 83 条による制裁金が科されない違反行為に適用されるその他罰則関する規定を定め、それらの罰則を科すために必要なあらゆる措置をとらなければならない。それらの罰則は、実効的、比例的なものであり、かつ抑止的効果を有するものでなければならない。

1. Member States shall lay down the rules on other penalties applicable to infringements of this Regulation in particular for infringements which are not subject to administrative fines pursuant to Article 83, and shall take all measures necessary to ensure that they are implemented. Such penalties shall be effective, proportionate and dissuasive.

2. 各加盟国は、第 1 項に従って採択した国内法の規定を 2015 年 5 月 25 日までに、また、それらの規定に影響を及ぼすその後の改正についても、遅滞なく、欧州委員会に通知しなければならない。

2. Each Member State shall notify to the Commission the provisions of its law which it adopts pursuant to paragraph 1, by 25 May 2018 and, without delay, any subsequent amendment affecting them.