資料２

個人情報保護制度に対する関心事項

亜細亜大学法学部　加藤隆之

１　課徴金制度の導入について

『日本で導入すべきではない。』

・GDPR には、制度上も運用上も、多くの問題がある（参考資料参照）。

・個人情報の誤用によって、既に、個人情報取扱事業者は、刑事罰、損害賠償、顧客からの信用喪失など、既に十分な制裁を受けている。権利の重要性に鑑みて、制裁金を導入することは、均衡を失している。

・GDPR のような制度を導入すれば、たったひとつの漏えい事故によって、企業を壊滅的に追い込むことが少なくとも理論的には可能となるため、企業への萎縮効果は甚大なものとなる。

・公正取引委員会による課徴金制度では、必ずしも不当な利得の簒奪が目的とされているわけではないと解されているようであるが、この目的を完全に欠落させた場合、行政による課徴金制度が際限なく広がる可能性がある。

・憲法上、他に重要な人権は多く存在する。にもかかわらず、個人情報保護のみ特別扱いする理由が不明である。他の権利侵害に対しても、課徴金制度を導入すべきということになりかねない。

・プライバシー権が人権であることは、先進国では共通の認識があるが、個人情報保護が人権であると明確に謳っているのは EU 基本権憲章（EU Charter of Fundamental Rights）第 8 条しかないのではないだろうか（もちろん、個人情報保護がプライバシー権に関係することについては誰も否定していないが）。

２　域外適用・執行について

『政府レベルで行うことが不可能ではないと思うが時間がかかるので、まず、民間レベルでの取組みを促進すべきである。よって、日本で域外適用の規定の制定に積極的であるべきではない。』

・GDPR のように域外適用の規定を設けることは理論的に可能だと思うが、その執行は、相手国の協力がない限り難しい。また、各国の人員や予算の状況、言語などの点で、円滑な協力を得られるか疑問がある。さらに、相手国の法律で域外適用の規定がないとお願いするだけになってしまう。

・個人データの越境的な問題については、Accountability の考えを基礎として（ややこの考えも公的機関を対象とするなど、その対象を広げすぎであるように感じているが）、APEC や OECD の枠組みを利用し、世界的な標準を設けるように促進すべきである。このような枠組みのもとでは、各国の法律が全事業者を対象に一律規制する

のではなく、越境移転を行う事業者のうち、積極的に同標準を遵守しようという事業者に対してルールを提供するのである。他方、消費者にとって、こうした企業が認識できればよい。

3　個人情報保護条例について

『法律による一本化をすべきである。』

・現在の地方公共団体の数はおよそ 1750 であり、そのうち、すべての地方公共団体が個人情報保護条例を制定しているかは不明であり、かつ、審議会が恒常的に開催、運営されているところは、ある程度の規模の自治体に限られるであろうが、それでも、日本全体での行政コストは非常に大きい。ほとんどの審議会で同じような議論が繰り返されているように思われる。とすれば、典型的な二重行政といえるのではないだろうか。

・個人情報保護という目的について、地域の特殊性があるとはあまり思われない。仮に、地域の特殊性がわずかに存在するとしても、それが法律レベルで吸収できないか検討すべきである。

4　個人情報の利用について

『他人の個人情報を利用したインターネット上の（収益）行為に対して、場合によっては、厳しい規制を設けるべきである。』

・いわゆるリベンジポルノ法は、プライバシー侵害及び名誉権侵害の程度が大きいことが明らかであることから制定されたが、「私事性的画像記録」であることが求められている。すなわち、「性的」な記録以外には適用されないのである。しかし、それ以外のプライバシーを侵害する記録、たとえば、性的記録を含まない盗撮行為に対しては規制が比較的緩やかであり（軽犯罪法や条例は存在する）、事実上、被害者の救済方法としては損害賠償請求しかないが、コストなどの点で、現段階では非現実的な手段である。

・とりわけ他人の個人情報を収集し、それをインターネットすることを業としている事業者に対しては、厳しい規制が必要であるように思われる。このような場合は、本人の同意の範囲を通常超えるものであり、適法性を見出し難いのではないだろうか。いわゆる名簿屋対策が語られることがあるが、それで対応できないケースが見受けられる。たとえば、学生が各教員の授業に意見を持つことは自由であるが、それが「みんなのキャンパス」というサイトで、大学の教員の授業評価が全国で誰でも見られるということとは話が異なる。

・以上の点は、個人情報保護法の範疇を超える可能性も十分あるので、個人情報保護委員会でのみ対応できることではないことは承知している。

（参考資料）

GDPR の制裁金制度

1　制裁金制度の概要

EU の個人データ保護制度としては、1995 年にデータ保護指令が制定され[1]、同指令のもとでは、制裁金の定めについて規定がなかったが、加盟国の国内法の多くでは、同制度を採用し制裁金を科していた。しかし、その運用や額については、各国でばらつきが相当あった。たとえば、イギリスやスペインの制裁金の上限は高額であるが、ルーマニアやスロバキアのそれは低額であることが知られていた。そこで、2018 年 5 月 25 日から施行されている加盟国を直接義務づける「一般データ保護規則」（General Data Protection Regulation、GDPR）[2]では、こうした各国間の差異を解消するために、規則違反に対する制裁金制度を導入した。すなわち、GDPR83 条では、一定の条文に違反する行為に対して、制裁金[3]を科すことができる旨を定めている。そして、同条では、制裁金の対象を民間団体とし、公的団体に対して制裁金を科す制度を設けるか否かついては、各国の裁量事項（7 項）としている。なお、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（2 項本文）。

公的団体にも制裁金制度の意義を認めるべきであると解する見解は、データ保護法に違反した公的団体に制裁金を科せば、その組織の予算は削られることになるから一定の効果が認められるとしている。他方、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主張する見解もある。それゆえ、いずれの見解をとるかについては、各国の判断に委ねられることとなっているのである。

いかなる GDPR 違反行為が制裁金対象となるかについては、次の通りである。

（a）1000 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）

---

[1] Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data.

[2] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 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.

[3] administrative fines の訳語については、課徴金という訳語をあてる専門家も多いが、ここでは、日本に存在する課徴金制度とは異なるものではないかという問題意識を明らかにするため、より広い意味を持つと考えられる制裁金の訳語を用いることにする。

・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　取扱い行為の記録（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　監督機関に対する個人データ侵害の通知
（Notification of a personal data breach to the supervisory authority）
・34 条　データ主体に対する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監視団体の適切な措置
（41 条、Monitoring of approved codes of conduct）

（b）2000 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 条、6 条、7 条、9 条における、同意の条件を含む基本的取扱い原則
・12 条～22 条におけるデータ主体の権利
・44 条～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

2　制裁金制度の問題点

以上のような GDPR の制裁金制度の特徴は、（a）広汎性、（b）曖昧性、（c）高額性の 3 点にまとめることができる。すなわち、規制対象行為の範囲が極めて広汎（広汎性）であり、その内容も曖昧である（曖昧性）[4]。ほぼ、すべての個人データの取扱いに関する行為が制裁金の対象となり得るし、また、具体的に何を怠れば制裁金が科されるのか不明瞭なことも多い。たとえば、個人データの管理者や取扱者は、監督機関と協力しなければならないとされているが（31 条）、監督機関と協力というだけでは、その行為規範が極めて不明瞭である。

また、データ保護違反があった場合、管理者らは、監督機関やデータ保護主体にその旨を通知する義務があるが（33 条、34 条）、この義務も必ずしも明確なものではない。というのも、監督機関への通知は、その侵害によって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を除くとなっているからである。このリスク判断を誤れば、高額な制裁金が科され得る[5]。同様に、データ侵害が自然人の権利及び自由に対して高リスクを引き起こし得る場合、データ主体へ通知が義務付けられている。このリスクが高いのか低いのかについての判断を誤れば、高額な制裁金が科され得る[6]。同様のことは、プライバシー・バイ・デザインとプライバシー・バイ・ディフォルトについて定める 25 条などについてもいうことができよう。

にもかかわらず、これらの義務に違反すれば、1000 万ユーロ（1 ユーロ 120 円で計算すると 12 億円）又は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が科される。さらに、忘れられない権利（17 条）については、それを GDPR が明文化されたことは多くの議論を呼んでいるが、この権利を保護しない行為に対しては、2000 万ユーロ（1 ユーロ 120 円で計算すると 24 億円）又は全世界年間売上高の 4%のいずれか高額な方

---

[4] 同旨、Sebastian Golla, Is Data Protection Law Growing Teeth? The Current Lack of Sanctions in Data Protection Law and Administrative Fines under the GDPR, Journal of Intellectual Property, Information Technology and E-Commerce Law (JIPITEC) Volume 8, Number 1, (2017) 77.

[5] GDPR70 条 1(g)では、欧州データ保護会議が、33 条 1 項で定める管理者又は取扱者が個人データ侵害の通知を要求される特定の状況に関して、ガイドライン、提言及び最良準則（best practices）を公表することとなっており、これによって一定の基準が示されることになるだろう。実際上の運用では、これが公表されるまで、同条違反を理由に制裁金が科されることはないように思われる。

[6] 同様に、GDPR70 条 1(g)では、欧州データ保護会議が、34 条 1 項で定める自然人の権利及び自由に対する高リスクが発生し得る個人データ侵害の状況に関して、ガイドライン、提言及び最良準則を公表することになっている。そのため、前注と同様のことが言えよう。

を限度として制裁金が科される。ところが、いかなる場合にデータ主体からの削除要請に応じるかについては、依然として不透明な点が多い。

ちなみに、グーグル年間売上高は、近年、10 兆円を超える規模となっており、仮に 10 億円の 4%とすると最高 400 億円までの制裁金を科すことも可能となる。もうひとつの上限となっている 200 万ユーロ（24 億円）どころではない額を科すことができるのである。実際に、フランスのデータ保護機関である「情報処理及び自由に関する全国委員会」（Commission nationale de l'infromatique et des libertes）」（CNIL、クニール）は、2019 年 1 月、グーグルに対しておよそ 62 億円もの制裁金を科したという。

もっとも、GDPR 違反があった場合、制裁金を科すか否かは、リサイタル 148[7]及び 83 条に従って検討される。すなわち、同規則の違反行為に対して直ちに、制裁金を科すという判断がデータ監督機関からなされるわけではない。

リサイタル 148 の第 2 文では、些細な規則違反の場合、若しくは、科される制裁金が不均衡な負担を自然人に与える可能性の高い場合には、制裁金ではなく戒告文書（reprimand）が出されるべきであると定められている。また、83 条 1 項では、制裁金の賦課が、比例的（proportionate）、実効的（effective）、抑止的効果を有する（dissuasive）なものでなければならないと定められている[8]。

そして、制裁金を科すか否かを検討するに際しての検討事項についても、リサイタル 148 及び 83 条 2 項で詳細に列挙されている。たとえば、83 条 2 項(a)では 、個人データ取扱いの性質、範囲及び目的、影響を受けたデータ主体の数、並びに、彼らが被っ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、当該違反行為の故意又は過失の特徴などを考慮すべきとなっている（(k)まで続く）。このように、様々な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ことになっている。

---

[7] In order to strengthen the enforcement of the rules of this Regulation, penalties including administrative fines should be imposed for any infringement of this Regulation, in addition to, or instead of appropriate measures imposed by the supervisory authority pursuant to this Regulation. In a case of a minor infringement or if the fine likely to be imposed would constitute a disproportionate burden to a natural person, a reprimand may be issued instead of a fine. Due regard should however be given to the nature, gravity and duration of the infringement, the intentional character of the infringement, actions taken to mitigate the damage suffered, degree of responsibility or any relevant previous infringements, the manner in which the infringement became known to the supervisory authority, compliance with measures ordered against the controller or processor, adherence to a code of conduct and any other aggravating or mitigating factor. The imposition of penalties including administrative fines should be subject to appropriate procedural safeguards in accordance with the general principles of Union law and the Charter, including effective judicial protection and due process.

[8] この基準は、EU 法違反の事件において加盟国によって課される規制や制裁に関する欧州司法裁判所（European Court of Justice）の法域に依拠したものであると指摘されている（Sebastian Golla, 75）。

さらに、29 条データ保護作業部会[9]では、2017 年 10 月に、「制裁金制度の適用及び規定に関するガイドライン」を出した[10]。その文書の導入部分では、データ保護ルールの一貫した執行は、調和の取れたデータ保護体制にとって重要であり、制裁金は本規則で導入された新しい執行制度における中心的な要素であることが謳われている。

このように、GDPR の制裁金制度は、データ監督機関の広い裁量を制約し、データ保護法の規制対象となる者に対して、違反行為が制裁金対象となるのかの予見可能性を失わせないように努めていることが窺われる。

だが、それが成功しているか、また、成功するかについてはかなり疑わしいといわざるを得ない。GDPR の条文の意味は、依然として極めて曖昧で不明確だからである。制裁金制度の運用が今後といかなる方向へ行くのかについては、誰も予測できない状況になっている。

さらに、デンマークとエストニアの法制度は、本規則で定める制裁金を認めていない。デンマークでは、権限を有する国内裁判所によって刑罰として罰金が科され、また、エストニアでは、監督機関によって軽罪手続の枠組みにおいて罰金が科される（リサイタル 151）。アイルランドでも、制裁金制度は採用されていない（この制度の採用が憲法違反となるかについては争いがある）。

したがって、いかにして EU 加盟国の間で、一貫性のある調和のとれた執行が実現するとは到底思えないのである。

---

[9] 29 条作業部会は、GDPR の制定により、「欧州データ保護評議会」（European Data Protection Board）に組織改編された。

[10] Guidelines on the application and setting of administrative fines for the purposes of the Regulation 2016/679 (WP 253) (Adopted on 3 October 2017).