GDPRの適用に伴う本学の対応の検証

髙　橋　　司

Verification of correspondence with application of “GDPR”

Tsukasa Takahashi

１．はじめに

所謂モノのインターネット（IoT、Internet of Things）の進化が目覚しい昨今、個人情報が簡単に手に入るようになったこともあり、個人情報を保護することの重要性が以前にも増して不可欠のものとなった。ビッグデータが利活用されることによる新たな経済成長も見込まれており、尚のこと重要性が上がった。そのような中、2017年５月30日に、改正個人情報保護法[1]が施行された。個人情報保護法の成立後約10年経っての大改正であった。

この個人情報保護法の改正については、個人情報保護委員会の設置と監督権限の付与、個人情報自体の再定義や要配慮個人情報[2]についての規制、オプトアウト[3]による提供手続きの厳格化や匿名加工情報[4]の利活用、そして、小規模事業者の要件[5]の撤廃、が大きな改正点として挙げられる。特に、小規模事業者の要件撤廃により、個人情報取扱事業者の範囲が拡大されたことで、大企業のみならず中小企業も含めて事業を行う者は、常に個人情報保護を意識せざるを得なくなった。また、グローバル社会の浸透に伴い、外国にある第三者への情報提供や、外国で個人情報等を取り扱う場合など、海外との個人情報のやり取りについても規制されることとなった。

個人情報保護法改正は大々的に取り上げられたが、海外でもその傾向は変わらない。2018年５月25日、

1　個人情報の保護に関する法律（平成15年５月30日法律第57号）

2　個人情報保護法第２条第３項「本人の人種、信条、社会的身分、病歴、犯罪の経歴、犯罪により害を被った事実その他本人に対する不当な差別、偏見その他の不利益が生じないようにその取扱いに特に配慮を要するものとして政令で定める記述等が含まれる個人情報をいう。」

3　言語の意味は不参加、脱退を意味する。個人情報に関するオプトアウトとは、メールなどを受け取りたくない者は個別に拒否することで、当該メール等を受け取らないことができるようにすることを言う。送信を申し込むのではなく、送信されることが前提の上で、送信を拒否することができる権限のことを指す。

4　特定の個人を識別することができないように個人情報を加工し、当該個人情報を復元できないようにした情報のこと。個人情報保護委員会HP（https://www.ppc.go.jp/）より。

5　個人情報保護法上、法律上の義務を負うのは、個人情報データベース等を使用する個人情報取扱事業者とされている。この個人情報取扱事業者に当たるのは、改正前は、個人情報を5,000件超有する事業者のみとされていたが、本改正によりこの条件が撤廃されたため、原則として個人情報を有する事業者は、情報数が5,000件以下であっても法の適用対象となる。

欧州連合（EU、European Union）の一般データ保護規則（GDPR、General Data Protection Regulation[6]）が施行された。EUが制定したものであるが、EUだけが対象となる訳ではなく、EU加盟国28カ国[7]と、欧州自由貿易連合（EFTA、European Free Trade Association）のアイスランド、リヒテンシュタイン、ノルウェーを加えた欧州経済領域（EEA、European Economic Area）31カ国の個人に商品やサービスを提供する者全てに適応されることになる。

日本においても、EUに進出している国は2016年度で2,631社あるが[8]、それらの会社はもとより、現地法人が無かったとしても、IoTを通じてEEA域内の個人とのやり取りをする会社であれば適用対象となってしまう。

日本でもGDPRの適用について多少取り上げられたものの、やはり対岸の火事の印象なのか、そこまで報道で取り扱われたように筆者には思えない。2018年７月に、日本のホテル業界で日本初のGDPR違反のおそれがあると報道されたが[9]、それも大々的に、しかも長期間の報道がされてはいなかったと記憶している。だが、制裁金など罰則規定もある以上、きちんと理解しておかないと多大な影響を受けるおそれも有る訳で、それが他人事でなくなったのは、去る2019年１月21日の報道であろう。これは、フランスにおける情報保護当局である、情報処理及び自由に関する国家委員会（CNIL、Commission nationalede l'informatique et des libertés）が、アメリカのIT大手のグーグルに対し、個人情報を収集する際、利用者に明確な情報を提供しなかったことはGDPR違反に当たるとして、制裁金５千万ユーロの支払いを命じた、とするものであった。GDPR違反の制裁は、これが初めてということもあるが、その金額の大きさと、その対象が世界的に身近な企業であることは衝撃的であり、GDPRの重要性が改めて認識されることとなったと言えよう。特に、グーグルはGDPRの対応をしていたと主張していたようであるが、それだけを見ると、単に企業として対応している、というだけでは駄目だということである。つまり、規則に沿った対応をし、かつ、それが一般的に認識されるようなぐらいの水準のものでなければ、誰もが規定違反に当たってしまう可能性があるということを示唆している。

2019年２月１日午前０時に、日本とEUの経済連携協定（EPA、Economic Partnership Agreement）が発効され、日本が約94%、EUが約99%の品目で関税を無くすこととされた[10]。今後、日本とEUとの間で貿易が盛んになれば、当然、このGDPRの適用を受け得る会社は増大することが予想される以上、今こそGDPRについて再度認識を深めなければなるまい。特に、国家による企業秘密の開示請求の禁止や、データのやり取りには関税をかけないこと、知的財産では著作物の保護期間を著作者の死後70年に延長すること、など幅広い分野の規定が盛り込まれていることは、個人情報の保護は手厚いものとしながらも、自由なデータの移転が可能になるという点で、今まで以上に個人情報保護の重要性が増したと考えられる。本稿では、GDPRの中身を簡単に、かつ、大まかに見ながら、本学における影響について検証していく。

---

6 「Regulation（EU）2016/679」と表記されることもある。より詳細に、「個人データの取扱いに係る自然人の保護及び当該データの自由な移転並びに指令95/46/ECの廃止に関する欧州議会及び欧州理事会規則（REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL 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）」

7 イギリスはEU脱退が決まっているが、発効日当日には未だ離脱していないため、現状適用を受けている。離脱後は直接の適用対象からは外れることになるが、恐らくその流れは変わらないであろう。

8 第47回海外事業活動基本調査結果　第２－１表、経済産業省　平成30年５月公表

9 これは、欧州のホテル予約サイト「ファストブッキング」のサーバーが不正アクセスされ、欧州からの宿泊者の氏名等の個人情報が流出した事件である。同サイトに業務委託をしていたプリンスホテルや藤田観光など日本国内の401箇所のホテル等から合計33万件弱の個人情報が流出したとファストブッキング社より報告されている。

10 即時に関税が０とされるものもあれば、数年後に関税０とする項目もある。

２．GDPRの中身

EUにおいて、個人情報保護は欧州連合基本憲章（The Charter of Fundamental Rights of the European Union）第８条第１項、欧州連合の機能に関する条約（The Treaty on the Functioning of the European Union）第16条第１項にて定められている[11]。尚、個人情報保護自体が基本権（プライバシー権）として定義されているのが特徴である。

EUでは、1995年10月に「個人データ取扱いに係る個人の保護及び当該データの自由な移動に関する1995年10月24日の欧州議会及び理事会の95/46/EC指令」が採択されて、当該指令を元に各国で独自の個人情報保護体制が採られることとなるが、加盟国毎の個人情報保護の違いや、EU全体としての個人情報保護の強化などの意図もあって、当該規則の制定に至ったと言われている[12]。

GDPRは、一般に、個人データ（personal data）の取扱い（processing）と移転（transfer）についての規則であるといわれる。よって、GDPRが個人データや取扱い、移転をどう捉えているかを知る必要があろう。

GDPRの第１条～第３条では、「本規則は、個人データの取扱いと関連する自然人の保護に関する規定及び個人データの自由な移動に関する規定を定める。」「本規則は、自然人の基本的な権利及び自由、並びに、特に、自然人の個人データの保護の権利を保護する。」「EU域内における個人データの自由な移動は、個人データの取扱いと関連する自然人の保護と関係する理由のゆえに制限されることも禁止されることもない。」として、対象や目的を定めている。

GDPRにおける個人データの定義としては、第４条第１項において「「個人データ」とは、識別された自然人又は識別可能な自然人（「データ主体」）に関する情報を意味する。識別可能な自然人とは、特に、氏名、識別番号、位置データ、オンライン識別子のような識別子を参照することによって、又は、当該自然人の身体的、生理的、遺伝的、精神的、経済的、文化的又は社会的な同一性を示す一つ又は複数の要素を参照することによって、直接的又は間接的に、識別されうる者をいう。」とされている。また、同様に取り扱うこと自体も定義化されていて、同条第２項にて「「取扱い」とは、自動的な手段によるか否かを問わず、収集、記録、編集、構成、記録保存、修正若しくは変更、検索、参照、使用、送信による開示、配布、又は、それら以外に利用可能なものとすること、整列若しくは結合、制限、消去若しくは破壊のような、個人データ若しくは一群の個人データに実施される業務遂行又は一群の業務遂行を意味する。」と規定されている。そして、要配慮個人情報については、第９条第１項で「人種的若しくは民族的な出自、政治的な意見、宗教上若しくは思想上の信条、又は、労働組合への加入を明らかにする個人データの取扱い、並びに、遺伝子データ、自然人を一意に識別することを目的とする生体データ、健康に関するデータ、又は、自然人の性生活若しくは性的指向に関するデータの取扱いは、禁止される。」とされている[13]。そして、個人データを有する者として、管理者（controller）と処理者（processor）の二つも定義している。第４条第７項で「「管理者」とは、自然人又は法人、公的機関、部局又はその他の組織であって、単独で又は他の者と共同で、個人データの取扱いの目的及び方法を決定する者」を、

---

[11] 個人情報保護委員会HP（前掲４）によるGDPRの日本語仮訳より。以下、条文の掲載は、当該仮訳を載せている。（https://www.ppc.go.jp/files/pdf/gdpr-provisions-ja.pdf）

[12] EUには、規則、指令、勧告、決定、意見と幾つか種類があり、加盟国での法的拘束力が異なってくる。従前の指令は加盟国で個別に法律を制定しなければならないが、規則であれば、各国での立法は不要であり、また、規則であれば直接法的拘束力を及ぼすことができる。

[13] 有罪判決及び犯罪と関連する個人データについては、第10条に規定されている。

同じく同条第８項で「「処理者」とは、管理者の代わりに個人データを取扱う自然人若しくは法人、公的機関、部局又はその他の組織」と定義している[14]。

GDPRに違反した場合は制裁金が課せられているが、これは、事業者以外の政府機関や事業団体も負わされる。軽度の違反（管理義務違反、処理者の義務違反、データ保護措置義務違反、データ侵害の報告義務違反、監督機関への協力義務違反など）と、権利侵害に基づく違反（データ保護原則に関する義務違反、第三国移転に関する保護措置義務違反、監督機関の命令等に対する違反など）の場合で罰則が異なる。前者であれば、1,000万ユーロか、全世界年間売上高の最大２%、のいずれか大きい方の金額を上限とする罰則となり、後者であれば、2,000万ユーロか、全世界年間売上高の最大４%のいずれか大きい方を上限とする罰則となる。

３．GDPRにおいて求められる対応

現状、GDPRの適用を受けないとすれば、EEA域内に拠点が無く、EEA域内の個人データをEEA域内から処理や移転などをすることが皆無の場合のみとなる。逆に言えば、それ以外の場合には、EEA域内拠点は勿論のこと、EEA域外であってもGDPRの適用対象となり得るということである。具体的に、日本の企業等にGDPRが直接適用される範囲は以下の状況が考えられる。

①EEA域内の拠点が収集した個人データを日本の本社で管理している場合

②日本の本社が、EEA域内の拠点とは別に直接EEA域内に商品・サービスを提供したり、行動を追跡したりしている場合

③現地に拠点がない日本企業が直接EEA域内に商品・サービスを提供したり、行動を追跡したりしている場合

上記三つの状況であれば、EEA域内の拠点は勿論のこと、日本の本社でもGDPRの適用を受けることになる。現状、①のように、EEA域内の拠点から日本の本社に個人データを移管する場合、EUから十分な保護措置を講じていると認められることが必要になる（GDPR第45条）[15]。一方、アメリカの企業については、プライバシーシールド[16]によって移転が可能となっている[17]。

GDPRに罰則がある以上、当然に罰則が適用されないような対応をせねばならない。具体的には、取扱いの原則を遵守しつつ、適法になっていれば良く、規則の第５条と第６条を満たすことが必要となる。

---

[14] 先の、日本のホテルの情報流出で言えば、実際に個人データを扱っていたファストブッキング社が処理者であり、業務委託をしていた日本のホテルが管理者という位置づけになる。拠って、処理者であるファストブッキング社から管理者であるホテルに情報が移転しているとなれば、GDPRのいう「移転」に当たり、結果、GDPRの域外適用を受けることとなるおそれがある。

[15] 現在、EUから十分性認定を受けている国は、2018年３月現在で、アルゼンチン共和国、アンドラ公国、イスラエル、ウルグアイ東方共和国、英領ガーンジー島、英領ジャージー島、英領マン島、カナダ、スイス連邦、デンマーク自治領フェロー諸島、ニュージーランドの11カ国・地域である。2019年１月23日に日本も十分性認定される旨の採択がなされた。欧州委員会と日本の個人情報保護委員会と相互に同等性を承認する決定の採択をし、同時に法的効力も発効された。但し、この十分性認定については、決定採択後から２年後に最初の監査を、その後４年に一度の頻度で監査が続けられることとなった。同日、日本の個人情報保護委員会は、「個人情報の保護に関する法律に係るEU域内から十分性認定により移転を受けた個人データの取扱いに関する補完的ルール」を公表した。尚、日本も同時採択という観点から、EEA域内の国について、日本の個人情報保護が同等の水準にあると認める国としている。

[16] EUとアメリカとの間で結ばれた個人情報移転フレームワークのことで、2016年２月２日に合意、同年８月１日より発効されている。マイクロソフトなど1500社が署名。

[17] 2018年７月５日に、欧州議会において、プライバシーシールドの枠組みを停止すると決議された。

規則第５条には、適法性・公平性及び透明性、目的の制限、データの最小限化、正確性、保存の制限、完全性・秘密保持性、説明責任が規定されており、取扱う際の基本原則となっている。一方、規則第６条には、取扱いに関して同意を得る場合、データの取扱いが契約の履行上必要となることや契約締結前に取り扱われる場合、EU法、或いは加盟国の国内法上の法的義務を遵守する場合、自然人の生命に関する利益を保護する場合、公共の利益や公的な権限の行使の場合、管理者に正当な理由がある場合、のいずれかに該当すれば適法となる旨規定している。

この点、同意の取得は、日本においても適法とされる根拠となる。同意についてはGDPRの第４条第11項で定められているが、要件をまとめると、①同意が自由になされていること、②同意の範囲が特定されていること、③処理の目的と内容について十分な説明を受けた上で同意されていること、④同意したことが明確であること、⑤声明か明確な意思表示でなされていること、とされている。同様に、規則第7条で同意の条件として、①管理者が同意を受けたことが立証できること、②同意の要請は、分かり易く、容易にアクセスできる形式で、平易な言葉を用いられており、他の事項と明確に区別されていること、③同意をいつでも撤回できることが明示されていて、かつ、撤回も同意と同程度に容易であること、④契約の履行にとって不要な個人データの処理への同意が契約条件となっていないこと、が挙げられている。つまり、同意を得る手順や方法が分かり易いものでないと、同意を得たことにならないため、注意が必要となる[18]。

そして、他にGDPRの特徴として挙げられる点の一つとして規則第17条に規定されている「忘れられる権利（right to be forgotten）」である。これは、インターネットにおける削除の権限を想定していると言われており、自らの個人データを削除してもらえる権利のことである。つまり、個人データが不要となったり、違法に処理されたり、同意が撤回されたりした時などに削除を要請すれば、公益等の例外が無い限り管理者は削除しなければならない義務を負うこととなる。

次に、企業等がGDPRに違反しないように個人データを移転するにはどうすべきか。この点、適切な安全管理措置が採られていることが求められるが、その措置として、標準契約条項（SCC、Standard Contractual Clauses。又はSDPC、Standard Data Protection Clausesともいう。）を締結すること、若しくは、規則第47条に規定されている拘束的企業準則（BCR、Binding Corporate Rules）の締結のいずれかを採ることがGDPRにおいては求められる。前者は、欧州委員会が決定したデータ移転契約のひな型で、ひな型で定められた項目[19]の削除は認められていないが、自主的に追加することができ、個人データの移転をGDPR上適法化するためのものである。一方で、後者は、グループ企業内における個人データの国際移転に関する企業内の規則をいう。BCRについては企業内規則ではあるが、これを締結するには、主要拠点を置く国の監督機関の承認を得なければならない。よって、グループ内外問わず使用できることや、承認等の手間がないことから実用性があるのは前者のSCCであろう[20]。

また、規則第37条により、データ保護責任者（DPO、Data Protection Officer）を選定しなければならない。特に、主たる業務がデータの使用の場合には、当該データ保護責任者を定めておく必要がある[21]。

また、規則第35条の規定により、個人データの処理が自然人の権利と自由に高いリスクを及ぼす場

---

[18] 先述したグーグルの制裁金については、同意の手段や方法が明確でないという理由で課せられたと報道されている。
[19] 具体的には、データの種類や内容、移転の目的、データの受領者、機微データの有無などを記載しなければならない。
[20] SCCには、EEA域内の管理者とEEA域外の管理者との間で締結するものと、EEA域内の管理者とEEA域外の処理者との間で締結するもの、の二種類がある。前者は、移転の目的ごとに締結する必要があり、後者は、処理の内容ごとに締結する必要がある。
[21] 但し、必ずしも社内の人間でなければならない訳ではなく、外部委託も可能。

合[22]には、データ保護影響評価（DPIA、Data Protection Impact Assessment）を行わなければならない場合もある。これは、リスクの高い個人データ処理について、リスク軽減対策を評価する手続きを指す。

そして、先述した、規則第45条が、十分性認定に基づく移転について規定している。これは、欧州委員会が十分なデータ保護の水準を確保していると決定した第三国、第三国内の地域又は一若しくは複数の特定の部門、又は国際機関に個人データの移転を行う場合は個別の許可を要しないとするものである。

上記で、大まかに内容の一部を取り上げてきたが、まずは個人データのたな卸しに始まる現状把握が真っ先に求められる対応であろう。そして、その上で、リスクの高いものから対策を練っていき、ITのセキュリティ対策や適法となるためにデータ主体による同意[23]や、SCCの締結をすることなどを行っていくこととなる。

４．GDPR適用に伴う本学への影響と対策

前章までで、GDPRの内容を見てきたが、それが教育機関に与え得る影響を考えてみる。まず、個人情報を扱う点で言えば、教育機関だからこそ沢山の個人情報を抱えている。単純に、学生の氏名、性別、住所、生年月日だけでも、個人の特定には十分な情報があり、更には、家族の情報（両親の有無、両親の氏名、生年月日、職業など）もあれば、奨学金等を得ている学生については親の年収までも学校が捕捉している事になる。その上、場合によっては、卒業生の情報も保持していることもあるし、それ以外にも、教職員の個人情報も抱え込んでいる。歴史のある学校や、多くの在校生を抱える学校であれば、その数は計り知れない。教育機関そのものが、個人情報を扱う場面が一般の企業等よりも多く、また、機微情報を扱う機会も多い以上、その保護の重要性は一般企業等よりも真摯に受け止めなければならないのである。

そこで、個人情報がどのような形で取得し、処理・移転され、保管されているかを把握することがまずは必要であろう。学内で、どの部署が、どのような個人データを保有・保管をし、どのように使用しているか、はきちんと整理しておかなければならない。その上で、GDPRで求められている個人データに関する管理者を誰にするか、何か問題があった時、つまりインシデント対応の手順や学内のエスカレーションフローの整備などをマニュアル化し、教職員全員に周知徹底するなども必要である[24]。学校によっては、職員と教員とで情報の非対称性がある場合も多いため、危機意識が異なってくることも起こり得る。学校全体としての個人データのたな卸しや対策を見直していくことが、全ての教育機関に求められると考える。

では、上記の前提を元に、GDPRの適用が本学にどのような影響を及ぼすであろうか。まず、直接的に、EEA域内とのやり取りを行うことは考えにくいため、その点について適用を受けることは無かろう。本学では、海外との関わりだけで言えば、短期留学や、海外語学研修、ボランティアセンター主催のボランティア活動などが海外渡航を伴う活動として挙げられるが、現状、短期留学や海外語学研修は、提

---

[22] 例えば、信用履歴に伴う自動貸付審査や、雇用主による業務車両の位置情報監視、従業員の私的通信を含むPC使用状況の監視を行う場合が挙げられている。

[23] 同意を得ることは日本の個人情報保護法でも求められる対応であるが、日本のそれよりも同意の有効性については厳しい扱いがなされている。例えば、従業員の健康診断の情報など会社として必要な情報であったとしても、対等な立場ではない者の同意は必ずしも有効とはならず、結果、会社が従業員との間で同意を得たことにならないケースも想定される。

[24] GDPRにおいては、情報漏洩発生時、72時間以内に関係当局への報告義務を課しており、これに違反した場合は先述した制裁金が課される。

携校のあるアメリカ合衆国が相手先となるため、直接EEA域内の個人データを扱うことは考えにくい。

また、ボランティア活動についても、海外ボランティアは、国などの第三者が立案したプログラムに乗じる形で参加しており、本学が海外の者と直にやり取りをする機会は無いため、EEA域内の個人データを扱うことも無い。そのため、やはり直接的な適用はないものと考えても差し支えない。

一方で、本学が取引をしている外部の企業等が、GDPRの適用を受けることは当然有り得るし、容易に想像がつく。新潟県内の企業に絞ったとしても、当然その余地は免れない。それらの企業が、GDPRの適用を受けるに当たり、自社の個人情報保護体制について何らかの規制強化をした場合には本学にも影響が出てこよう。しかしながら、企業のGDPRの適用は、あくまで企業が保有する個人データに関する扱いであって、当該適用に伴う規制を本学に強要するものではない。（但し、本学の個人情報保護体制が整っているか、などの検証・確認は当然に行ってくるであろうが。）よって、これに伴う影響も少ないと見て取れる。

では、逆に、どのような場合に、本学においてGDPRの直接適用が有り得るだろうか？これは、つまりはEEA域内の個人データを本学で直に取り扱う状況を考えれば良い訳だが、想定されるケースとしては、留学生の募集や、教職員の採用についてであろう。

本学においても、留学生の募集を行っているが、その際、入学希望する者から募集要項等の請求があった場合、手渡しならともかく、郵送する場合であれば当然、当該希望者の住所氏名等を把握した上で要項などを送付することになる。その際、当該希望者がEEA域内に住んでいる個人であれば、当該個人の住所氏名などから個人データを捕捉できるし、また、実際に入学するとなれば、当該個人の生年月日や家族情報なども当然に収集することになる。そうなると、留学生が本学を何らかの形で知り、入学に至らなくとも資料請求等をした時点で、本学としてGDPRの適用を受けると考えられる。それが、仮に1件だけだとしても、また、稀にしか起こりえないとしても、適用を受けるとなった段階で、本学としてはGDPRの適用体制ができていることが当然に求められてしまうことになる。

留学生の受入体制がある以上、本学としても、GDPRの適用に沿った個人情報の取扱いを再度検証しなければならない。これは、本学、つまり短期大学部のみならず、大学も留学生受入の要項を持っている以上、大学としても対応せねばならないことである。上記のことは、教職員の採用についても同様のことが当てはまるであろう。特に、教員については、外国籍教員を採用することもあり得る以上、留学生募集よりもその緊急性は高く、至急に採用に関する個人データの取扱いについて見直す必要があるのかもしれない。

一般的に、学校法人は何処も個人情報を扱う件数が甚大なため、適切な管理方法を採っているであろうし、そのための教職員の教育等も行われているはずである。本学でも、HPでのプライバシーポリシーの公表を始め[25]、教職員の教育など種々の対応は行われている。しかしながら、日本の個人情報保護法や、いわゆる番号法[26]の対応のみでは、GDPRの適用に必ずしも適合する、若しくは求められているレベルに達しているとは限らないため、より高度な対応が求められる。

最後に、見方を変えて、個人データを扱う場面について再考してみると、PCの利用に伴うネット環境においても問題が生じそうである。ネットのセキュリティを考える際に、インシデント発生時にどのように検知し情報を共有していくか、クラウドを使用している場合にはどのようなデータがあり、どう保護するか、他にマルウェア対策や、不注意によるデータ流出時のリスク軽減などが行われているかを

[25] http://www.n-seiryo.ac.jp/privacy/
[26] 行政手続きにおける特定の個人を識別するための番号の利用等に関する法律（平成25年５月31日法律第27号）のこと。

確認することが必要である。

本学は、学生へのPC貸与を行っており、その際、無線LANの環境も整備していて、学内でのネット接続を可能としている。あくまで貸与しているPCからの接続のみに限定しており、携帯電話やその他の端末からのアクセスは可能としていないため、誰もが使えるフリー Wi-Fiなどの無線LANよりはセキュリティは高いと言えるかもしれない。しかしながら、PCを貸与し、学内無線LANに接続できる権利を与えている以上、それを使用する学生の個人情報保護の意識も高めていくことも本筋としては必要になるはずだ。情報処理の授業等で、その点について講義しているが、今後更に重点的に扱っていくことが重要だと思われる。それは、学生が社会に出てからも必要不可欠なことである以上、教育の一環でもある。このご時勢、何処からどのような形で情報が漏れるか想定しにくいのであるから、学生についても個人情報保護の重要性を認識する機会を適宜設けていくことを検討していかなければならない。個人データの取得が同意を前提としている以上、同意を与えることの危険性を理解させること、また、SNSなどで簡単に個人情報を載せること自体の危険性を理解させること、などを社会に出る前に、そして知る機会を多く与えることで、日常的に意識を高めさせることも学校の役目でもあろう。

5．おわりに

本稿では、大まかにGDPRを俯瞰した上で、最終的に、本学への影響について検証してみた。当然、これは検証で終わるのではなく、実際に大学も含めた学校法人全体として対応せねばならないことである。現在、外国人労働者の受入拡大を図り、入管法[27]改正も謳われており、将来的に、留学生の受入を拡大していくことも、少子高齢化が益々侵攻している日本においては必要不可欠のことで、それは本学も避けられない事実である。だからこそ、現状、GDPRへの対応を早期に行うことによって、海外への情報発信に繋がることも期待できるのではなかろうか。

筆者の知る限り、学校法人で、GDPRへの対応を銘立っているところはない。当然、個人情報保護体制はどこの学校法人でも対応しているであろうが、何かしらの個人情報の漏洩があった場合、GDPR適用云々の前に、そもそも日本における個人情報保護法違反等が問題となるであろう。それを考えれば、敢えてのGDPR適用のためだけの個別の対応というのは必要ない、と考えるのも無理はない。だが、だからこそ、きちんとしたGDPR対応を行い、それを公表していくことが、日本国内のみならず海外も視野に入れた本学において必要なのだと考える。

同意の明確性が欠如していると判断されるだけで制裁金が課せられる現状を鑑みると、改めて、個人情報に纏わる問題や対策を見直していかねばならないことを再認識するべきであろう。

また、日欧EPAの発効は、今後日本において経済効果の増大が期待されている。これは学生にとっても、他人事でなくなることも意味している。先述した通り、学生のうちから個人情報保護の重要性を認識し、社会に出た際に面食らわないよう、また、社内外で個人情報保護の重要性を提唱できる様になれるぐらいに、授業等でも積極的に教授していくことも必要であろう。単に、教職員だけの意識高揚に留まらず、学生にまで拡げることが求められていると考える。

[27] 出入国管理及び難民認定法（昭和26年政令第319号）のこと。政令とはなっているが、法律と同等の効力を有している。

参考文献等（前掲以外）

・藤原靜雄「日本とEUの個人情報保護法制の比較」、ジュリスト1521号（有斐閣、2018.7）14 ～ 19頁
・『欧州GDPR全解明』、日経BPムック、2018. 6
・宮下紘『EU一般データ保護規則』、勁草書房、2018. 5
・足立照嘉・ヘルマン・グンプ著『GDPRガイドブック―EU一般データ保護規則活用法』、実業之日本社、2018. 5
・経済産業省HP「EU：一般データ保護規則、十分性認定等の動きを踏まえた産業界の取り組みと課題」（JIPDEC主催第18回データ流通促進WG ～国境を越えるデータ流通の促進）