

情報サービス業の進展と各国のプライバシー関連法/ 制度の変化が我が国のプライバシー関連法/制度に与える影響

岩 出 和 也

ICTの進歩により、消費者は多くのネットワーク経由でサービスを利用している。特に、この数年間でクラウドサービスの利用率は劇的に向上し、特定のデバイスに縛れることなくデータを運用するようになった。

その一方、その情報サービスを取り巻く制度は未だ未成熟な状態にあり、さらに、国境等の法/制度の境界を越えたデータの移動に対して、各法/制度間の整合性が取れていないのが現状である。データ移動に関しての法/制度の中でよく取りざたされるのが、プライバシー関連の法/制度である。その中でも、影響の強いものに、EUデータ保護指令があるが、現在、EUデータ保護規則への格上げが議論されている。同時に米国においても消費者プライバシー権利章典が発表され、大きな変革の時を迎えているといえる。

一方、日本の国際的な枠組みでの存在感は低調であり、国際的に通用するスキームを整備することだといえる。本論文では、国内外の法/制度を比較すると共に、国際的な枠組みへの参加の必要性と方向性を示す。

keywords : EUデータ保護規則、消費者プライバシー憲章、個人情報、情報サービス、越境した法執行

目 次

1. ICTの活用の進展と境界を越えた情報移動に関する課題
 - 1.1 先行研究の整理
 2. EU、英米、国際的な取り組みの法/制度の変化の兆し
 - 2.1 EUデータ保護規則案 (General Data Protection Regulation)
 - 2.2 米国における消費者プライバシー権利章典 (A Consumer Privacy Bill of Rights)
 - 2.3 英国 midata project
 - 2.4 国際的枠組み
 3. 国内の政策動向
- おわりに
参考文献

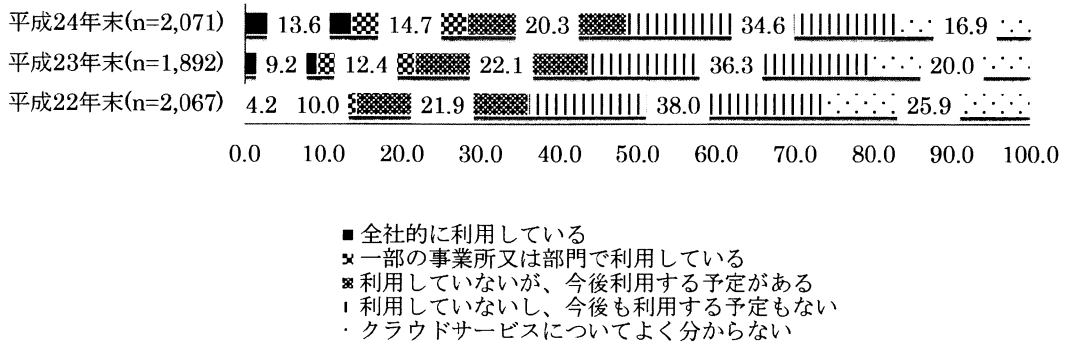
1. ICTの活用の進展と境界を越えた情報移動に関する課題

ICT技術の進展と普及により、クラウドサービス等、法/制度の境界を越えた情報の流通は極めて容易となった。これは、消費者にとって特定の

デバイスに縛られず、情報を運用することが可能になり、大きな利便性をもたらしている。さらに、これらの情報サービスは無料か、安価に提供されることがあり、これまで主流であったデバイス、パッケージ商品双方を必要とするモデルに対して競合する存在になっている。

クラウドに代表される情報サービスを利用することにより、個人の利便性が向上することはもちろん、企業や公的機関においてもコストを削減することが可能となる。しかし同時に、情報流失等の問題も生じ、自由な情報流通と情報活用によるイノベーションと、情報保護の双方を確保する必要がある。特に、企業や公的機関は多くの個人情報を保有しており、情報サービスの利用に関してより高いレベルでの対応が迫られている。例えば、企業のクラウドサービス利用状況(図表1)を見てみると企業が導入に積極的であることが解る。

また、公的機関においても、2009年のエコポイント制度の申請システムや静岡県等の災害時等広域連携システム等にクラウドサービスを導入してい



出典：平成 24 年通信利用動向調査, P19, 図表3-11

図表 1 国内企業のクラウドサービスの利用状況

る。

個人、企業が利用を進める中、ITCの特性上、生じた問題が、国境等の境界を越えて発生する可能性は、他の財、サービスに比べて著しく高い。また、消費者とサービス供給者の所在地と、サービス供給者が指定する管轄裁判所、データセンターの所在等、複数の法/制度に跨った形でサービスの需給が行われるため、問題が生じた場合の法/制度の迅速なエンフォースメントに問題が生じることがある。さらには、消費者は現実にデータセンター等の所在を確認することなく、どの法/制度へコミットメントしているかという認識を失う傾向にある。現実に、SNSやクラウドサービスで大きなシェアを誇る企業の多くは米国のシリコンバレーに存在しており、先にあげたエコポイントや静岡県の災害時等広域連携システムを提供するsalesforceは米サンフランシスコに本社がある。salesforceは日本国内におけるサービスについて、準拠法を日本国法に指定し、担当裁判所を東京地裁に指定しているが、Googleは利用規約において、アメリカ合衆国カリフォルニア州サンタクララ郡内に所在する裁判所を指定しており、GoogleSuggestの名誉棄損裁判に対する履行拒否等の法執行に問題が出ている事案が存在する。法執行に問題が出ている事案が存在する。

供給者が、国外でサービスを行う場合、該当国の司法に従わなければならないが、情報サービスの分野においては、変化が速く、新しいサービス形態の普及に対して十分な法/制度が準備できて

いないのが現状だといえる。このような背景と、後述するEUデータ保護指令等との不整合の中で、日本政府及び日本の法/制度の影響力が低下してきているといえる。情報サービスを利用する際、挙げられるリスクには、供給が停止してしまうことが挙げられる。停止の要因としては、一つは経済的理由による事業撤退があり得るが、別に押取等法的なリスクも考えられる¹。供給が停止された場合、データセンター内にある消費者のデータが失われてしまうことも十分に考えられ、法/制度の不整合はデータセンターの司法による押取や、通信遮断等のリスクを伴う。円滑な利用を妨げない為には法/制度のハーモナイゼーションが望まれる。

1.1 先行研究の整理

情報サービス産業について、プライバシー関連の法/制度についての研究は、喫緊の課題であり、かつ情報サービス業は成長が望める分野であるため一定の研究の蓄積がある。公官庁の調査報告として総務省（2013）、消費者庁（2008）等があり、諸外国の制度と国際的枠組みを紹介している。

新保史生(2001)は、EU、米国間の差異とセーフ・ハーバー協定について検証している。また、EUデータ保護規則案については一般社団法人電子情報技術産業協会情報政策委員会（2012）が調査報告を行っている。

生貝直人（2011）は、欧米の制度について、実例を用いて詳細に検討すると共に、共同規制とい

う考え方を基に、情報社会における規制のあり方について検討している。共同規制は、政府による直接規制や、私人による自主規制ではなく、政府と民間が共同して規制を行うものあり、情報社会における新たなガバナンスの可能性を指摘している。

一方、我が国の法/制度との整合性において、独立した第三者機関の設置について疑問を呈する動きもある。小向太郎（2011）は、憲法上の問題を指摘し、第三者機関の強制力に疑問を呈している。

本論文は、これらの先行研究を基に現状を総括的に捉えると共に、新たな視点から展開されつつある英国midata project、国際的な枠組みでの取り組みを加えて検討する。

2. EU、英米、国際的な取り組みの法/制度の変化の兆し

実際に、多くの情報が境界を越えて流通する中、各国の法/制度は接近しつつあり、また、国際的な枠組みでの対処が生まれつつある。この議論において特に影響の大きいものは、プライバシー関連の法/制度であり、それぞれの枠組みの域外での情報の保管、移動について規制している。そのなかで影響力の大きいEUデータ保護指令、米愛国者法については城川俊一（2013）が詳しいが、本章においては、EUデータ保護指令を規則へ格上げする法案や昨今進展している国際的な枠組みについて記述する。

プライバシー関連の法/制度において、その先駆けとなったのは1980年のOECDプライバシーガイドラインであり、具体的には①収集制限の原則②データ内容の原則③目的明確化の原則④利用制限の原則⑤安全保護の原則⑥公開の原則⑦個人参加の原則⑧責任の原則の8原則が提言されている。主眼は越境執行協力に関する国際的枠組みの創設である。越境協力体制は、2007年のプライバシー保護法の執行に係る越境協力に関するOECD勧告で改めて促している。以下の各法/制度は、このOECDプライバシーガイドラインの影響の下で策定されてきた。

2.1 EUデータ保護規則案

(General Data Protection Regulation)

EUデータ保護規則案の基となったEUデータ保護指令（95/46/EC）により、EUを構成する28か国は、域内における個人情報の取り扱いと、域外への移動を厳しく統治してきた。域内においては、EUデータ保護指令により国内法の整備を義務付けている。域外については、EU加盟国と同じ水準を満たしていることをEUデータ保護指令第25条及び第26条の適用（WP12 5025/98）により審査し、国と地域²を十分に認定国とし、個人情報の移動を認め、それ以外の第三国への移動を禁じている。充分性の代表例としては、実効性のある個人情報保護の包括法³と独立的な監督機関（第三者機関）の設置が挙げられる。例外として、米国は包括法がないものの、米欧セーフ・ハーバー協定⁴を結びEU域内と、米商務省の認めた企業に対して個人情報の移動を認めている。

EUデータ保護指令は1995年に制定したものであり、以下に述べるように現実との齟齬をきたし始めている。そのため、EUデータ保護規則案は2010年前後から改訂の準備を始め、2012年に欧州議会に提出された。その背景は、技術進歩による①データの共通や収集の規模の拡大②企業及び公的機関による大規模な個人データの活用③個人による個人情報の公然とした公開が世界規模で展開されていることであるとしている。これらは、1999年時点では見られなかった、クラウドサービスや、ビックデータ、SNSが急速に拡大してきたことを念頭に置いているといえる。個人情報に関しての取り扱いについて、明確なオプト・インを求めており、暗黙の同意を認めておらず、また、同意を撤回できる権利の保障義務の追加、忘れられる権利の精緻化（第17条）及びデータ・ポータビリティの権利（第18条）が保障されており、情報の取り扱いについて、個人の権利が重視される傾向にある。

また、EUデータ保護指令では、国内法を通じての規制であったものを、規則に格上げし、EU法により、直接適用し制度の一本化を図っている。EUデータ保護指令下では、域内であっても加盟国ごとの国内法への対応が必要であり、監督機関

図表2 日本、米国、EUの個人情報保護関連法/制度

| | 日本 | 米国 | EU |
|-------------|------------------------------------|--|-------------------------------|
| 第三者機関 | 独立した監視機関がない、複数の省庁が所管(15省庁) | 独立した監視機関が無い、複数の機関が所管(3機関) | 設置を義務付け |
| 第三国移転 | 第三者、第三国への提供に対して寛容 | 保険衛生、金融に関して国内法での運用が明記(HIPAA プライバシー規則、GLBA) | データ保護指令により、域内と米国、充分性認証国に限る |
| 企業等の規模 | 中小規模の企業が対象外 | 全企業 | 全企業 |
| 利用の規定 | ダイレクトマーケティング・プロファイリング等に対する拒否の規定が緩い | 「Do Not Track」に代表されるオプト・アウトの権利 | ダイレクトマーケティングにおけるオプト・アウトの規定が存在 |
| 情報漏洩等に関する義務 | 情報漏洩時の報告・連絡義務がない | 州ごとの個別に存在、連邦法化が検討 | 罰金を含めた報告義務 |
| 司法による救済 | 司法による救済に関する権利の規定がない | 明記されていない | 司法による救済の権利が存在 |
| 利用に関する認証形態 | オプト・アウト | オプト・アウト | オプト・イン(例外有) |

出典:経済産業省(2012)、消費者庁(2008)、White House(2012)、European Commission(2012)参考で作成

への報告義務もあるため、その作業ごとにコストが発生することになった。制度を一元化することにより、コストを引き下げることが可能になると考えられる。

日本への影響としては、EUデータ保護指令では、EU域内の設備でデータ処理を行う場合のみ適用を受けていたものが、EUデータ保護規則では域外の設備であっても、EU居住者のデータ処理を行う管理者に対して規制が適用されるものの、EUの保護基準への充分性の申請について、国単位ではなく⁵、民間部門のみや、特定の産業のみでの申請が可能になったため、充分性の認証を得られる機会が増加したといえる。

2.2 米国における消費者プライバシー権利章典 (A Consumer Privacy Bill of Rights)

米国においては、1980年のOECDガイドラインを基に、2012年に消費者プライバシー利用章典(以下、章典)を発表した。立法勧告段階で立法には至っていないが、EUデータ保護指令、EUデータ保護規則とは異なった視点から策定が行われている。

章典は、①個人のコントロール②透明性③背景情報の尊重④セキュリティ⑤アクセスと正確性⑥

適切な範囲での収集⑦説明責任の7つの要素で構成されている。

米国がEUと大きく異なるのが、EUが個人情報に関して厳格なオプト・インを指向しているのに対して、基本的にオプト・アウトの姿勢を示していることだ。米国FTCは「Do Not Track」(以下DNT)の概念を提唱し、事業者によるインターネット上の追跡を拒否できる権利を示している。DNTにより、消費者は行動ターゲティング広告の為に、事業者が情報を収集することを拒否することが出来る。また、米国FTCは2012年の報告書「急速に変化する時代における消費者プライバシーの保護」において、消費者の選択を必要としない個人データを規定している。これにより、企業は自社のサービスや、公共目的であれば、明確な同意を得ずに個人情報の使用が可能になっている。これらは、明確にオプト・アウト方式を指向したものだといえる。

一方、「急速に変化する時代における消費者プライバシーの保護」では、オプト・インが必要な情報⁶についても記載されており、一部強化の方向が表れているのも事実である。

米国、EU、日本の個人情報保護の法/制度を整理すると、図表3のような特徴を持つ。

2.3 英国 midata project

英国ビジネス・イノベーション・職業技能省（以下、BIS）が2011年に発表した「Consumer empowerment strategy published」において設置された、midata project（以下、midata）は他の制度と大きく異なった性質を持っている。

midataは、BISと Google、British Gas、Lloyds TSB、O2などが中心となり推進しており、消費者が企業の持つ個人情報にアクセスすることを可能にする制度である。企業が、個人情報を利用してマーケティングを行うのではなく、個人が企業の持つマーケティングに利用できる情報にアクセスする権利を保障している。これにより、消費者はより合理的な判断が可能になるという概念の下でmidataが設置された。初期段階として、金融、携帯電話事業、エネルギー産業、小売り業を対象に運用されており、自発的な参加がなされない場合、法律により強制的に参加させることを2012年に発表している。実際に電力に関しては企業・規制改革法が2013年に議会で承認されている。また、2014年3月をもって、進捗状況を確認し、さらなる対応を検討するとしている。

2.4 国際的枠組み

1980年のOECDプライバシーガイドライン以降、国際的な枠組みの構築が進められてきた。実効性のある制度として整い始めたのは2000年代中盤以降に入ってからである。本節では、代表的な国際的枠組みについて検証する。

（1）コミッショナー会議

コミッショナー会議は1979年以降年一回開催されている、各国・地域の情報保護機関から構成される情報保護及びプライバシーに関する国際会議である。この国際会議は、国及び地域の情報保護に関する第三者機関を正式なメンバーとしており、それ以外にも、政府機関関係者や学者、民間の専門家が参加する。2005年に「グローバル化した世界における個人データ・プライバシーの保護：多様性を尊重するユニバーサルな権利7（The protection of personal data and privacy in a globalised world：a universal right respecting diversities）」が出される等、プライバシー関連

の法/制度に対して強制力こそ持たないものの、一定の影響力が存在する。ビッグデータ等、先端的な分野についても議論、決議が行われる。登録を行う出席する公開セッションと、認可を受けた第三者機関の関係者のみが出席を認められる非公開セッションがあるが、日本は第三者機関が存在しない為、非公開セッションや決議に参加できていない。

（2）APEC CPEA（APEC 越境プライバシー執行：Cross border Privacy Enforcement Arrangement）

APECの枠組みの中で運用される、国境等を越えて発生する個人情報等の問題に対して、被害を受けた主体の存在する国のプライバシー執行機関⁸が、供給主体の存在する国のプライバシー執行機関の援助を受けて法執行する体制のことである。参加単位はプライバシー執行機関であり、米国FTC、オーストラリア、ニュージーランド、香港、カナダ、日本、韓国、メキシコの各プライバシー執行機関が参加している。日本は2011年より参加している。

（3）APEC CBPR（APEC越境プライバシールールシステム：Cross Border Privacy Rules）

APEC CBPRは、APECのCPEAに参加していることを前提に、企業等の越境個人情報保護に係る取組に関し、2004年のAPECプライバシー原則への適合性を認証する制度である。プロセスとしては、①CBPRに参加している国がCBPRへの参加を申請し、承認を受ける。②プライバシー認証機関が各国の政府とプライバシー執行機関の審査を経て、APECの電子商取引運営グループ（ECSSG）、データ・プライバシーサブグループ（DPS）、共同監視パネルへ申請を行い認証を受ける。③認証を希望する企業等が、プライバシー認証機関へ適応度の審査を申請する。という流れである。認証を受けた企業等はAPECプライバシー原則への高い適応度が認められ、その企業等で問題が生じた場合はCPEAにより法執行を受けることになる。

企業の個人情報保護への適応度を認証するシステムで、米欧セーフ・ハーバー協定に類似しているといえる。米国とメキシコが認証機関の審査を

図表3 個人情報保護の国際的な取り組み

| 組織 | 名称 | 概要 | 参加 |
|-------------------------|---|--|--------------------------|
| OECD | OECDプライバシーガイドライン(1998) | プライバシー8原則を提唱し、参加国へ適応を求めた。 | OECD加盟国(32か国) |
| | プライバシー保護法の執行にかかわる越境協力に関するOECD勧告(2007) | 越境して発生した事案へのプライバシー執行機関間の協力体制の構築を求めた。 | OECD加盟国(32か国) |
| APEC | CPEA(国際法執行のための協力取決め:Cross border Privacy Enforcement Arrangement) | 国境を越えた個人情報の漏えい事案等での自国法にもとづく法執行に他国機関の協力を求めることのできる体制 | 8ヶ国のプライバシーコミッショナー(日本を含む) |
| | CBPRシステム(APEC越境プライバシールールシステム:Cross Border Privacy Rules) | CPEA参加国の中で、参加を認められたエコノミーの認証機関が、エコノミー内の企業等のAPECプライバシー原則への企業等の適合性を認証する制度 | 米国、メキシコ、日本(全て審査中) |
| データ保護プライバシー・コミッショナー国際会議 | | 各国・地域の情報保護機関から構成される情報保護及びプライバシーに関する国際会議。 | 40か国以上(日本はオブザーバー) |

受けており、日本は2013年6月に参加を申請した。

ここまで、欧州と米国における法/制度の変化の兆しと国際的な枠組みを見てきた。現実の進展に対して、各法/制度が未だ黎明期にあることが解る。昨今、米国とEUの法/制度は共同規制という形で接近しつつあるとの見方もある(生貝2011)。本論文において触れていない問題として、例えば、個人情報という概念にしても、曖昧であり、各法/制度で異なる理解をしていることが挙げられる。

国際的な取り組みの特徴をまとめると図表3のように整理できる。OECDのガイドライン、勧告、コミッショナー会議は拘束力が低く、実効性に疑問が残る。それに対して、実行力の伴うAPECのプログラムは参加国数が少なく、システムの運用についても実例がない、まさに揺籃期にあるといえる。

3. 国内の政策動向

ここまで、欧米のプライバシー関連の法/制度を見てきたが、本章では、日本における現状と、2013年6月に閣議決定された「世界最先端IT国家創造宣言」等を参考に政策動向を探る。

日本が、国際的なプライバシー関連の法/制度の領域で影響力を低下させている要因として、複

数の要因が考えられるだろう。第1に、日本の企業が提供するサービスの国際競争力は低いといえる(鈴木 2013b)。例えばSNSの分野でも、Google、Facebook、Twitter等、クラウドサービスでもDropbox米国企業のサービスが一般的になっている。これらの企業は多くの場合、本社の存在する米国の法律を準拠法に指定している。第2に欧米レベルの実効性を持つ包括的な個人情報保護法を持たないこと。第3に個人情報保護の第三者機関が存在しないことが挙げられる。この中で、特に問題なのは第2、第3の点であり、これらの改善が第1の問題への解決の道筋を示す可能性がある。

現在の日本の包括的な個人情報保護の法/制度は個人情報保護法があるが、EUデータ保護指令に比べて①独立した監視機関がない②個人情報取扱事業者の範囲が狭い③第三者、第三国への提供に対して寛容④ダイレクトマーケティング・プロファイリング等に対する拒否の規定が緩い⑤情報漏洩時の報告・連絡義務がない⑥司法による救済に関する権利の規定がない等の理由で十分性を満たしているとは言えない(電子情報技術産業協会2012)とされている。しかし、1980年OECDプライバシーガイドラインには、データ内容の原則が努力義務であることを除いて対応している。

しかし、第三者機関については、その不在が国際的枠組みの中で日本の存在感を失わせる要因となっている（新保2013、鈴木正朝 2013a）。現在、個人情報保護法によって規定された、プライバシー関連の所管がある省庁は15におよび、APEC CPEAには、そのすべての省庁が参加することで法執行を担保している。また、センシティブデータの定義においても、各所管の関係上表現が異なっており、範囲に差が生じている。国内の主体も、海外の主体も統一的な窓口すら存在せず、所管官庁の割り当ても複雑で解り難いことも問題とされている。そして、新保（2013）によると、第三者機関の役割は、法の執行だけにとどまらない。例えば、グレーゾーンにあるとされる情報の取り扱いについて、欧州の第三者機関は助言を行うことがある。2013年6月27日、日立製作所はJR東日本からSuicaのデータを提供し、ビッグデータとして事業化を行ったが、利用者などに対して十分な事前説明をしていなかったとして7月25日に事業を中断することになった。この事業はオプト・アウト方式による、データ利用の拒否を受け付け、再開を目指しているが、2013年9月に当面事業を見合わせると発表した。この事例において、問題になったのは、現実の使用状況と照らし合わせることで、追跡が可能になるのではないかという問題である。本件で提供される予定のデータは、「年齢、性別、職業」という組み合わせであり、センシティブデータには当たらないと考えられるが、現在、個人情報については政府が検討を進めている段階であり、不確実性からグレーゾーンになってしまう部分も多い。結果、企業等は委縮し、過剰反応により情報を死蔵することにつながってしまう。それに対して、欧州における第三者機関は、個人情報保護について横断的、包括的に所管しているため、国内外の個人情報関連の問題を総括的に整理、対応することが出来、グレーゾーンに何らかの指針を示すことが出来る（新保2013）。

一方、米国では、独立した第三者機関は持たないものの、オプト・アウト方式を取り、問題が発生した場合に対処することでグレーゾーンの問題に対処している。米国を発祥とする企業が大きな

存在感を示す現状を考えると米国のような政策を取ることも十分な価値が存在する。

政府は、「世界最先端IT 国家創造宣言」（総務省 2013）において、「パーソナルデータの利活用のルールを明確化した上で、個人情報保護ガイドラインの見直し、同意取得手続きの標準化等できるだけ早期に着手し、第三者機関の設置を含む、新たな法的措置も視野に入れた、制度見直し方針を年内に策定する」と、「我々は、これまでITの利活用が進まず、その成果を社会に十分に還元できなかった反省を踏まえ、ITに関する政府全体の戦略について、経済財政諮問会議、産業競争力会議、規制改革会議なども連携し、総合的に取りまとめていく司令塔として、高度情報通信ネットワーク社会推進戦略本部の呼称を「IT戦略本部」から「IT総合戦略本部」としたところであり、この「IT総合戦略本部」が、省庁の縦割りを排して、省庁横断的な課題について積極的に横串を通して、司令塔機能を発揮することが不可欠である。」としており、第三者機関創設の可能性が高まってきたといえる。

一方で、第三者機関が我が国において、十分に機能するかという点で疑問を呈する動きもある。小向（2011）では、憲法65条により、行政権は内閣に属していること、及び人事権が内閣にあることを理由に、実効性に疑問を呈している。また、政府から独立した機関への正統性の視点から国会のコントロールが直接に及ばない機関の正統性に問題が生ずる可能性を示している。さらに、精神的自由に対して、合憲性の推定が難しいことを指摘している。

また、勧告や命令について、独立した第三者機関の権限をどの程度担保できるかの問題があり、予算、人事の点で独立性の担保に問題が生じる可能性は存在する。さらに、所管する範囲や、国民及び企業等の利害関係者が膨大になり、調整が困難になり独立した第三者機関のみでの対応は、有名無実化する可能性も指摘できる。

しかし、現実公正取引委員会等の憲法65条から例外とされ、運用されている第三者機関も存在し、予算面での問題を克服出来れば、十分な機能を期待することが出来るといえる。

おわりに

本論文では、欧米のプライバシー関連法/制度と国際的な枠組みについて、その特徴を把握した。同時に、国際的にみて日本の法/制度の影響力を低下させている要因について指摘した。第1に実効性のある包括的な個人情報保護の法/制度がないこと。第1に個人情報保護の第三者機関が無いことである。

これらの状況は、国際的な発言力を著しく失う結果をもたらしていると言える。第2の独立した情報保護機関（第三者機関）は、権限や予算について問題が存在する。しかし、新保（2013）では、創設されれば、自ずと個人情報保護法下で15省庁にまたがっていた個人情報関連の所管が一元化され、行政プロセスの効率化や、一元的な窓口としての機能、国際的枠組みにおける発言力の向上等、利点が多い。速やかに第三者機関と、国際的ハーマナイゼーションのとれた包括的な個人情報保護法の改訂を行い、円滑な利用の保障がより強固となるようにするべきだとされる。第三者機関の創設は、国際的なハーマナイゼーションの一つであり、我が国の個人情報保護政策の国際化に重要な役割を果たすといえる。

一方、米国を発祥とする企業が大きな存在感⁹を示す現状を考えると米国のように、オプト・アウト型の政策を取ることは、自由な情報の流通がイノベーションの機会を抑制しないことを示しているとも言え、我が国の情報保護法/制度には、EU型のオプト・インによる保護強化と、米国型のオプト・アウトによる情報流通の促進について、十分な検討の上で情報の性質により、認証方式を分けるなどの方策の検討が望まれる。

英国、midataからは政府や公益事業者の持つ情報を、消費者である国民が活用することで、より合理的な選択をする援助の可能性を模索した試みであり、成果は未だ不明であるが、英国だけでなく、我が国を含め、各国が採用できうる制度であるといえる。

APEC CPEA、CPEAは、実行力の伴う制度であり、より大きな枠組みとしての運用の模索など、さらなる進展が、情報サービスの利用への一助に

なるといえる。

ICTに関係する事後的な制度整備は、情報の流通量とイノベーションの可能性を高めるが、同時に個人情報の流通によるリスクを高めることになる。しかし、事前に規制を設けることは、個人情報の保護に一定の成果を期待できる一方、イノベーションの可能性を抑制する可能性もあり、十分な検討が必要となる。情報通信分野は、技術進歩の速度が速く、新たなサービスが次々と現れるため、制度設計に関して迅速な対応が要求されるものの、それぞれの持つ意味について、拙速な結論を出すべきではないとも言える。

本論文では、主要国と国際的な枠組みについて、政府による関与を中心に検討した。現代日本で、情報サービスに触れないことは困難になっている。今後は安定的な供給への民間中心の関与や、供給に問題が起こった時に、補間或いは代替できるスキームの研究を行う。

[注]

- 1 具体的な例として、2009年4月2日テキサス州のデータセンター運営会社Core IP Networks LLCがFBIにより予告なしにすべての機器の停止を命令した事件が知られている。データセンターを利用していたすべての企業のサービスが停止しすべての消費者がサービスを利用不能になった。通信会社も利用していたため一時、緊急電話も不通になるという事態に陥った。米国愛国者法 (the Patriot Act) によるものだとも言われているが、村上康二郎 (2012) らは愛国者法によるものかは明らかになっていないとしている。
- 2 スイス、カナダ、アルゼンチン、ガンジー島、マン島、ジャージー島、フェロー諸島、イスラエル、アンドラの9つの国と地域となっている。カナダは包括法がなく、十分性が認められているのは民間部門のみ。これらの十分性認定国は、改定後も維持される見込み。
- 3 オーストラリアは包括法を制定し、十分国認定の申請をしたものの、①小規模事業者が規制対象外であること②一般に利用可能なデータが規制対象外であること、③データの第三国移転が規制対象外であること等を理由に十分性が認められなかった。
- 4 認証の原則は①通知②選択③第三者提供④セキュリティ⑤データの完全性⑥アクセス⑦執行の7つからなる。2010年にドイツがセーフ・ハーバー協定では不十分であると指摘している。(総務省2011、城川2013) 改定後も再度の交渉を求めるものの、維持される見込み。
- 5 ただし、申請は政府が行わなければならない。その際、

該当分野における保護法の十分性、行動規範と司法によるエンフォースメントが求められる。日本の十分性への問題として、統括的に個人情報を司るべき第三者機関の不在が挙げられるため、申請を行いやすくなったといえる。

- 6 データを収集した段階と、異なる目的でデータを使用する場合や、特定の目的でセンシティブ情報を収集する場合。センシティブ情報は社会的差別を生じる可能性のある情報を指し、人種、性別、本籍、出身地、思想や信仰などが挙げられる。
- 7 ①適法かつ公正なデータ収集及び取扱いの原則②正確性の原則③目的明確化・制限の原則④比例の原則⑤透明性の原則⑥個人参加、関係者のアクセス権保障の原則⑦無差別の原則⑧データ・セキュリティの原則⑨責任の原則⑩独立監視及び法的承認の原則⑪個人データの国際流通における十分なレベルの保護の原則⑫原則
- 8 プライバシー法の執行に責任を有し、調査の実施又は執行手続の遂行をなす権限を有する公的機関のことを指す。必ずしも横断的であったり、独立性が担保されている必要はない。
- 9 米国企業は、大きな存在感を示すとともに、米国政府の影響下にあり、対テロを名目とした米NSAによるPRISM問題が起こる要因となっている。Google、Microsoft等の企業に対するガバナンスとともに、その企業を要する国家に対する、正当性の証明に問題のある監視の抑制も国際的な取り組みとして必要とされる。

参考文献

Department for Business, Innovation and Skills, "Personal data"
<https://www.gov.uk/government/policies/providing-better-information-and-protection-for-consumers/supporting-pages/personal-data> 2013.9.6

European Commission,
 "Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on the protection of individuals with regard to the processing of personal data and on the free movement of such data" the Publications Office of the European Union, 2012
http://ec.europa.eu/justice/data-protection/document/review2012/com_2012_11_en.pdf 2013.9.3

European Commission, "Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation)" http://ec.europa.eu/justice/data-protection/document/review2012/com_2012_11_en.pdf 2013.9.3

White House, "Consumer Data Privacy in A Networked World : A Framework for Protecting Privacy and Promoting Innovation in the Global Digital Economy." White House, Feb. 23, 2012. <http://www.whitehouse.gov/sites/default/files/privacy-final.pdf> 2013.9.5

生貝直人 (2011)『情報社会と共同規制：インターネット政策の国際比較制度研究』勁草書房

一般社団法人電子情報技術産業協会情報政策委員会(2012)「EU データ保護指令改訂に関する調査・分析」http://home.jeita.or.jp/page_file/20120427161714_ljwGed1UnB.pdf 2013.9.15

城川俊一 (2013)「クラウド・コンピューティングの現状と課題—クラウド・コンピューティング—の導入におけるリスクと対策—」『経済論集』第38巻2号, P.57-P.67. 東洋大学経済研究会

村上康二郎 (2012)「クラウド・コンピューティングにおける個人情報保護の課題」『情報セキュリティ総合科学』第4号, P.118-P.119 (情報セキュリティ大学)

首相官邸 (2013)「世界最先端 IT 国家創造宣言」
<http://www.kantei.go.jp/jp/singi/it2/kettei/pdf/20130614/siryoul.pdf> 2013.9.10

消費者庁 (2008)「Ⅲ OECD・APEC・EU等の個人情報保護の国際的な取組」『諸外国等における個人情報保護制度の実態調査に関する検討委員会・報告書』P.223-P.272

新保史生 (2001)「個人情報保護制度の比較法的考察—米国・EU間におけるセーフ・ハーバー協定を中心に—」『憲法研究』第三三号, P.1-P.10 (憲法学会)

— (2013)「ネットワーク社会における個人情報・プライバシー保護のあり方」『基礎・境界ソサイエティ Fundamentals Review』第6巻, 第3号P.199-P.209 (電子情報通信学会)

鈴木正朝 (2013a)「わが国の個人情報保護法制の立法課題総務省」『第4回パーソナルデータの利用・流通に関する研究会 資料』
http://www.soumu.go.jp/main_content/000196107.pdf#search=%E9%88%B4%E6%9C%A8+%E6%AD%A3%E6%9C%9D+%E7%AC%AC%E4%B8%89%E8%80%85%E6%A9%9F%E9%96%A2 2013.9.23

— (2013b)「個人情報保護法制をめぐる最新課題」『情報通信学科 情報知財研究会 資料』

総務省 (2013)「パーソナルデータの利用・流通に関する研究会報告書～パーソナルデータの適正な利用・流通の促進に向けた方策～」
http://www.soumu.go.jp/main_content/000231357.pdf 2013.9.23