

個人情報保護をめぐる 新しい法制度体系の在り方に関する事例研究

高橋由利子[†] 木下貴史^{††} 横澤誠^{††}

近年、ネットワークの利用が多様化し、多くの主体が様々な方法で個人の情報を取得し、保持し、利用する機会が拡大している。本研究では具体的なプライバシー事象をクラウドコンピューティングなどの新しい情報技術の環境変化の中で考える。その上で日本、米国、欧州、アジアを対象に現行の個人情報保護体制の構造を再整理して、その得失の評価を行う。従来の国・地方自治体という縦軸、産業・分野別の横軸という二方向からの分析に加えて新たな視点を提案する。

The Best Legal System over Protection of Personal Information in the Information-Oriented Society

Yuriko Takahashi[†] Takafumi Kinoshita^{††}
and Makoto Yokozawa^{††}

Recently, as the use of network becomes diverse, every element in society becomes to get, hold or use personal information in various ways. In this research, we will examine privacy cases based on new coming technologies like cloud computing. The thing first to do is to put the structures of the present system of protection of personal information in order and to analyze them. The subject countries and regions are Japan, the United States, Europe, and Asia. Our goal is not only to analyze the present state considering the system of the government and the differences among industries as usual, but also to try to offer some different perspectives for the coming more highly information-oriented society.

1 はじめに

近年、情報通信技術の利用主体が多様化し、その取得、保持、管理について必ずしも統制が取れていない場面が拡大するに伴い、我々の個人情報が危機に瀕している。現行の法制度ではその保護は不十分であるが、同時に過度な保護は経済の発展と利用者の便益をも妨げかねない。本研究ではクラウドコンピューティングを例に挙げ、世界中で議論されている近未来のプライバシー問題を整理するとともに、日本、米国、欧州、アジアを中心とした現行の法制度の構造化を試みる。従来の方法に加え、法制度を新たな指標で分析することで、個人情報をめぐる種々の問題の解決に向けた新たな視点の獲得を目指す。

2. クラウドコンピューティング

2.1 クラウドコンピューティングとは

クラウドコンピューティングとは、近年注目を集めている新技術の一つである。インターネットのようなネットワーク、データ、計算資源、情報処理の機能を雲 (cloud) とみなし、ユーザが雲の中のリソースを自由に活用したり、雲から多様なサービスを受けたりすることができる仕組みのことをいう。このときユーザは雲の所在や内部の構造を知ることができない。クラウドコンピューティングには IT ベンダーが提供するサービスの種類に応じて SaaS (Software as a Service)、PaaS (Platform as a Service)、IaaS (Infrastructure as a Service) 等の種類がある。

2.2 クラウドコンピューティングをめぐる近年の動き

クラウドコンピューティングの導入をめぐるのは、世界中の企業や OECD のような国際的な組織でも数々の議論が巻き起こっている。その理由としてはこの新たな技術体系に対する期待と課題の両側面が有る。クラウドコンピューティングは、ソフトウェア技術と産業における最も影響の大きな変化であり、低コストで大規模かつ高機能なシステムの利用が即座に可能になることなど、多様な社会的イノベーションの核としても期待されている。ソフトウェア産業のみならず、他産業や政府、自治体、公共機関など社会全体においてクラウドコンピューティングが活用されれば、生産性を向上し新たな経済発展の原動力ともなりうる。

しかしながら同時にコスト削減の面だけにとらわれ、生産性の向上だけが目的となると、雇用や情報サービス市場規模の縮小、市場寡占によるユーザの利益の制限など、

[†] 京都大学大学院情報学研究科
Graduate School of Informatics, Kyoto University
^{††} 野村総合研究所
Nomura Research Institute

社会経済面で解決しなくてはならない問題点も数多く指摘されている。こうした課題の中でも特に懸念されているのがセキュリティとプライバシーの問題である。実際にクラウドコンピューティングをテーマとした国際的なシンポジウムも開催されているが、やはりそこでもプロバイダはユーザにデータが安全に取り扱われることをいかにして証明するのか、あるいはクラウドの中に蓄えられたデータにはどの国の法が適用されるのかといった問題が関心をあつめている。[1]また、図1はクラウドネットワークに関して行政に期待することというテーマで企業にアンケートをとった結果[2]であるが、これを見ても企業がクラウドコンピューティングのセキュリティ・プライバシー面に大きな懸念を抱いていることが読み取れる。

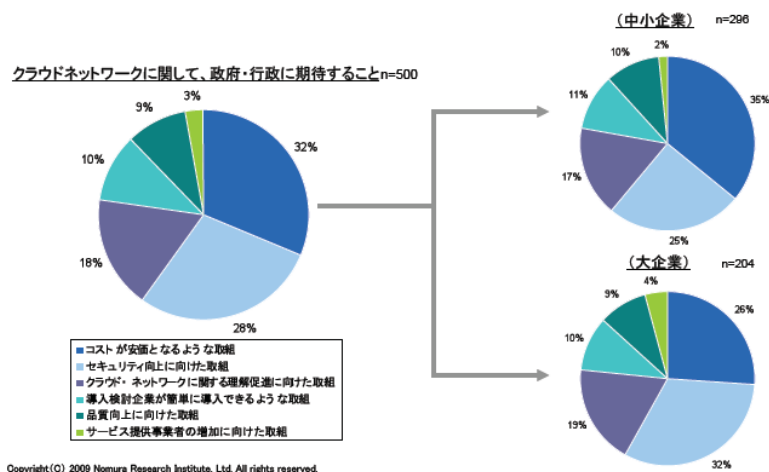


図1 企業のクラウドネットワークに関する政府・行政への期待 ([2]より引用)

また、図2はクラウドコンピューティングをめぐる諸問題のうちいくつかを様々な先行資料をもとに主観的に整理してみたものである。縦軸には社会的・政策的要請・ユーザ・個々の視点を、横軸には効用・課題を指標として採用した。この図からもわかるようにクラウドコンピューティングの利害は表裏一体のものであり、現時点では一概にその効果を断定することは難しいと考える。

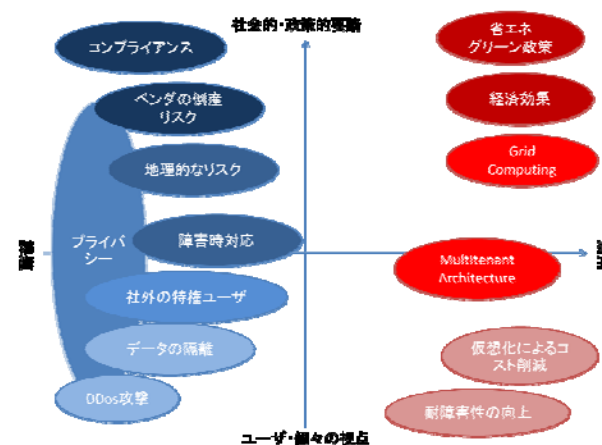


図2 クラウドコンピューティングがもたらすもの

3. プライバシーと個人情報保護

3.1 プライバシー

プライバシーの概念は国によって異なり、その法規定も多種多様である。わが国で初めてプライバシーという言葉が使われたのは1961年の「宴のあと」事件の判決文中である。プライバシーの権利は、我が国では以前はみだりに私生活を公開されない権利として、あるいは一般的にはひとりにしておかれる権利と解釈されていた（古典的プライバシー権, the right to be alone, Samuel D. Warren/ Louis D. Brandeis: The Right to Privacy, Harvard Law Review, 1890）が、時代が進むにつれて人権擁護の動きの中で自己の情報をコントロールする権利としてその範囲を広く捉える解釈（積極的プライバシー権, individual's right to control the circulating of information relating to oneself, Alan F. Westin: Privacy and Freedom, 1967）が一般的になった。情報化の進展に伴い、ネットワーク上の個人情報、実際に財産権の侵害の事例も増大するなど、その影響の範囲が広がり、全世界的にプライバシーの重要性の認識が高まっている。

3.2 個人情報保護をめぐる諸問題

人権としてのプライバシーの権利を保護する上で適切な個人情報の取り扱いは不可欠である。しかし法制度的な側面からの多くの議論を集約した結果、本研究では個人情報をめぐる諸問題の中でも、以下の四点が重要と考える。

- i). 法制度の構造論
- ii). クロスボーダーデータフロー
- iii). Alternative Dispute Resolution (ADR) と第三者機関
- iv). 責任分解と Internet intermediaries

3.3 個人情報保護制度の各国比較

個人情報保護の問題をより難しくしている原因の一つに各国の規制の相違ということが挙げられる。従来その体系は公的・民間部門の規制の態様に応じて、

セグメント方式(分離方式): 公的部門と民間部門とをそれぞれ別の法律で対象とする

セクトラル方式(個別分野別方式): それぞれの部門について、特定の分野で保護措置を講じる

オムニバス方式(統合方式): 一つの法律で国・地方公共団体等の公的部門(パブリック・セクター)と民間企業等の民間部門(プライベート・セクター)の双方を対象とする

の三種類に分類されている。[3]

本研究では新たに、先行資料を参考に様々な指標を加え、法制度の分析を行った。[4][5][6][7]結果の一部を表1に示す。この表はカナダ,アメリカ,イギリスの個人情報保護制度を第三者機関の存在,国際情報移転に関する規定,対象個人情報の種類及び情報の主体となる本人の権利を基準に比較したものである。

個人情報保護制度の比較を行う場合には、産業別や情報取扱者の主体別の規制が行われているかどうかにとどまらず、自主規制の範囲、センシティブ、目的外利用や直罰規定に関する規定の有無ないしその程度など、着目すべき点は非常に多岐にわたる。各国の法制度を比べると、規制の違いだけでなくどの部分に重点を置いているかまで判別することができる。例えば、カナダはプライバシー法(2002)の適用除外に関して一般適用除外 exclusion や個別的適用除外 exemption としての命令的個別適用除外と裁量的個別適用除外及び適用除外バンクを、PIPED 法(2002)に関して同法全体にかかる適用除外として属人的適用除外や対物的適用除外等を設けている。これは他国にはない目立った特徴であるが、このことからカナダは法規制の範囲を広くとり、適用除外によって個々の事態に対応するという構造を採用していることがわかる。他国に関してもそれぞれ独自の法体系や法解釈で個人情報保護体制を運用しており、それらの法の制定年度や改正の動向などが社会・歴史的背景と結びつくことは少なくない。

今後も世界的な経済や社会の流れに応じた個人情報保護が求められていくであろうが、もはや各国の法制度の違いを既存の三種類のモデルで完全に表現することは不可能なほど多様化が進んでいることは、表1からも容易に理解することができる。

表1 個人情報保護の各国比較 - カナダ・アメリカ・イギリス

	カナダ	アメリカ	イギリス
方式	セグメント	セクトラル	オムニバス
第三者機関	プライバシーコミッション(1)(63条) Oプライバシー法 PIPED法 苦情の処理・調査・裁判への付託 法的強制力 PIAに関する助言と監視 プライバシー問題に関しての場外への助言や 議会における法的検討に資する法・政策分析 プライバシーに関する権利や義務に際する 世論に関する意識や情報の提供 目標と懸念データ保護の問題を解決する ための国際的な協力 等	— 連邦取引委員会(独立の権限からも第三者機関とはいえない) 消費者保護に關する職務・権限 企業の人権の取扱いに關する不正の監視 金融機関の個人情報に關する規則の支離 訴訟に對する執行 消費者のプライバシー保護 等	情報コミッション(1)(63条) O個人データ保護法 情報自由法 法的強制力 行政 データ保護者の監督・立憲 普及・啓発その他の活動
国際情報移転	個人情報及び電子文書法 直接の移転は許していない EUの間でinert statement EUから(PIPED)はAdequate Levelとの判断	個別法で異なる HIPAA 国際協定によって運送される海外の医療ケア施設には適用される GLBA 宛先を跨ぎに行っている金融機関及び外国の金融に影響のある金融機関には、GLBAの遵守が義務付けられている WTOの間のサーフェーバー協定(Safe Harbor/2003)にデータ保護指令に對し 告知 承認 アクセス セキュリティ 第三者への提供 データの完全性 実施・執行	十分な保護のない第三国への移転制限(原則8原則) EU以外には情報の移転は原則禁止 多国籍企業はプライバシーポリシーを申請して 認定される必要があり後述 例外として裁判(ICOは事後対応),拘束力のある 企業ルール(ICO事前対応)
対象個人情報	プライバシー法 その対象のいかに問わず識別可能(Identifiable) 個人に關する情報	個別法で異なる FCRA: 消費者報告 (consumer report) HIPAA: 特定の個人を識別可能な健康情報(HI(Individually identifiable health information)) GLBA: 非公開個人情報 (nonpublic personal information)	自動処理データ 関連するファイリングシステムの一部として記録 される情報 (relevant filing system) 個人・データ個人情報 ex. 「怠けるである」「怠けるであるから版戻する」 は個人データ
本人の権利	プライバシー法 本人の自己情報開示請求権(12条1項) 本人の自己情報訂正請求権(12条2項) 訂正が認められなかった場合に訂正請求の 決定を当該情報に付せしめる権利(12条3項) 個人情報バンク(Personal Information Banks)や 政府による個人情報バンク外の情報の公開により、 求める情報がどこに存在するか政府が秘密に しようとする情報のカテゴリーは何か知ることができ るし開示の請求権もカナダ国民及び 移民は1976年によって永年認められた	開示 FCRA: 消費者に對する開示の際には、消費者報告機関は消費者 ファイルに記載されている事項の内容を開示する。単に消費 者報告の作成にのみ利用され、その他の目的に利用されてい ない情報源からの情報源についてはそれも開示しなければならない HIPAA: 開示に關する義務規定はない GLBA: 開示に關する義務規定はない各金融機関の自主性の中 でなされる 利用停止・消去 FCRA: 消費者に情報の上乗せについて争いが認められた場合 には、消費者報告機関は合理的な期間内に再調査し、その結果に 基づいて情報を訂正することが要求される。開示の結果、不正と された情報については消費者報告機関により削除される HIPAA: 訂正請求権が認められているが、利用停止や消去について は定められていない、異議機関との判断、州法の規定に受ける	個人データへのアクセス権(7条) 個人情報の取得元についても開示を請求できる 匿名又は匿名を与えられていない 取扱いを争いさせる権利(10条) デジタル・マーケティングの目的のための 取扱いを停止させる権利(11条) 自動決定に関する権利(12条) 一定の要件を満たさないことに関する権利(13条) 修正、削除、削除及び複製(14条) 質的権限及び手続(15条)

4. 現行法の限界

クラウドコンピューティングの実用化が進めば、あらゆるセキュリティ事象が想定されることは上述したとおりである。そのようなセキュリティの面での問題が発生した場合に、現行法ではどのような対処がなされるのか検討するためにここでは以下の事例を想定した。

事例: A 国籍のサービスプロバイダ (Sier) 企業 a が B 国の企業 b がもつ C 国にあるサーバ c にある情報を使ったクラウドコンピューティングを利用して D 国に住むユーザー d に対するサービスの提供を行った場合

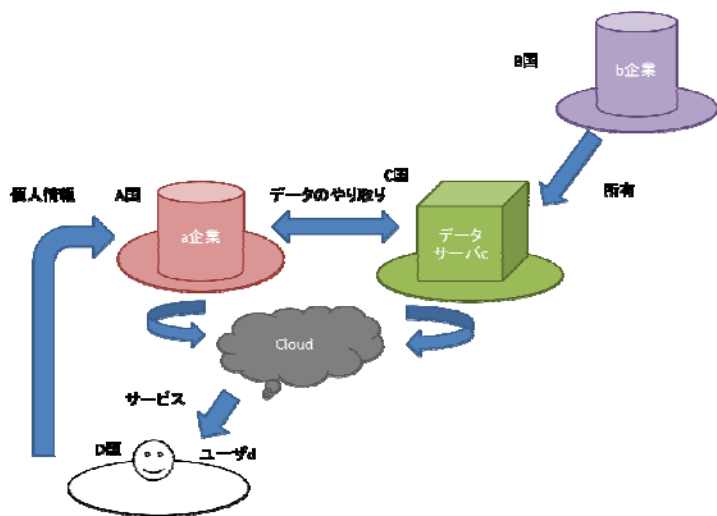


図4 本事例のイメージ図

図4は本事例における各関係を図式化したものである。

初めに、サービスを提供する過程でdの個人情報が流出したとする。本事例ではクラウドコンピューティングの中でii.)クロスボーダーデータフローが起こるため複雑な問題が発生する。まずクラウドの特性から情報が流出した場所を突き止めることから困難であることが前提にある。

次に例えばD国法が保護の十分でない第三国への情報移転制限を規定していたと仮定する。このときA国の保護は十分であるが、B国の保護が不十分でかつaやcやdがそのことにつき善意であった場合には、本事例における取引はD国法に違反したということになるのだろうか。そもそもA国籍の企業にD国法が適用されるのか、違反となった場合にはその損害の負担はどうなるのかというaとcのiv.)責任分解の問題が生じ得る。これはインターネットさらにいうならばクラウドが日常的に利用されるようになった社会において、企業の義務がどの程度まで広がるのかという問題に絡むが、その範囲が大幅に広がった場合には先にも述べたように法人はクラウドによる利益を手にすると同時に損害も被るようになるということである。またA国には独立した第三者機関があり、C国には類似のものがない場合の紛争解決はより複雑化するとと思われる。

このような問題が現代社会で起こった場合にはかなり深刻な状況を招く。その背景

としては各国のi.)法制度の構造論の個別性や国境をまたいだ紛争処理の解決を担う共通のiii.)第三者機関が存在しないことなどが考えられる。ADRの観点からも国ごとの第三者機関の有無や国際的に統一した機関の不在による不都合は少なくないだろう。

ここで再度、なぜクロスボーダーだと問題が増幅するのかという点に戻るが、このように、国際関係の中で個人情報保護を考える際の課題は以下のように整理される。

- 1) あらゆる国や地域の個人情報へのアクセスの機会が組み合わせ的に広がること
- 2) 各国の歴史や文化、政策や産業、環境の違いに起因する、規制の対象、方法、執行に関する多様性
- 3) 国内での事象以上に利用者、消費者から見た責任の所在、問題解決方法の不透明となること
- 4) 地理的にも物理的にも影響範囲が広範囲に及ぶ事で、個人情報に関する事象の事後対応が困難となること

以上のことから、現行法でクラウドコンピューティングに対応するには限界があることは明白である。とはいえ、個人情報の問題は保護と流通のバランスが最重要であり、法でどの程度まで規制を与えるべきかの判断は非常にむずかしいところであろう。しかし実社会においては近いうちに先の事例よりもさらに複雑かつ多様なケースが生じることは容易に予想できる。本事例を通して、テクノロジーの進歩が引き起こす負の側面への技術的ないし法的対応の重要性を再認識した。

5. 展望と課題

本稿ではクラウドコンピューティングを想定して、主にその中で発生することが予測されるプライバシー事象と現行の世界の法制度を勘案し、個人情報保護をめぐる諸問題の再整理を行った。さらに法制度の構造論に関しては新たな評価軸の提案も行った。近い将来訪れるであろう一層高度な情報化社会の到来に向けて、とるべき対策として以下の四つを提案する。

- 共通モデル型
あらゆる国や地域で同一の個人情報を対象に共通の規定となりうる規制のひな形を用意して、各国でそれをベースとした独自性の有る法制度構造を考える
予期される効果：統一的で安定している
解決すべき問題点：時代思潮や文化による考え方・感じ方の違い
- EU型
欧州でのEUのような仕組みを全世界的に広げる。センシティブ情報に関してはiを適用し、それ以外の個人情報については関係諸国の法制度を勘案して独立の第三

者機関が個別に対応できるようにする。プライバシー事象が生じた際に、関係国が不明の場合の対処法は事前に協議しておく。

予期される効果：各国の特性や応用（間接）的な個人情報に配慮した柔軟性を維持できる

解決すべき問題点：クラウドのような場合、企業やユーザが応用（間接）的な個人情報に関する予防措置をとることができない

・国際法型

国際法を整備する、すべての国で第三者機関を設置して統一的な組織を形成する

予期される効果：明瞭かつ統一的な制度となる

解決すべき問題点：反対国の説得、主権国家制への配慮、時間・費用等のコスト

・技術型

法整備だけでなく技術的な側面からの Privacy by Design やプライバシー強化技術 PET (Privacy Enhancement Technology)

予想される効果：法適用の厳しい範囲での保護

解決すべき問題点：コスト削減、国際協力、情報格差

以上をまとめて整理すると表 2 のようになる。

表 2 今後の対策の提案とその効果・問題点

	予想される効果	解決すべき問題点
共通モデル型	統一的,安定	時代思潮,文化の相違
EU型	柔軟性	曖昧さ
国際法型	統一的,安定	各国の合意の確保
技術型	法規制の補完	コスト,情報格差

急激な ICT の発展や不安定な現代の社会情勢を鑑みるに、今後個人情報をめぐる問題はより複雑化していくことが予想される。もはや独立の機関や一国の努力だけで対処できる状況ではない。したがって産官学民が連携して、法整備と技術的対応を組み合わせる、国内と国外の対策にグローバルに取り組む、あるいは事前対策と事後対応を同時並行で行う等、複数の措置による双方向的かつ複合的な対策を検討することが今後求められていくのではないかと考える。

参考文献

- 1) ICCP Technology Foresight Forum-“Cloud Computing: The Next Computing Paradigm?”-Agenda and Presentations, OECD/BIAC, 14 October 2009
- 2) クラウドネットワーク技術に関する諸外国の動向及び国内市場における利用意向分析, 総務省スマートクラウド研究会, 2009年12月16日
- 3) 堀部政男: 個人情報保護法の考え方, 科学技術・学術審議会生命倫理・安全部会ライフサイエンス研究におけるヒト遺伝情報の取扱い等に関する小委員, 2004年7月14日
- 4) 藤原静雄ほか: 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, 2008年3月
- 5) 堀部政男ほか: 情報公開・プライバシーの比較法, 株式会社日本評論社, pp.1-198 (1996)
- 6) 総務省・株式会社野村総合研究所: ユビキタスネットワーク社会の影の課題(大分類)に係る国際的政策動向, 2004年11月19日
- 7) 堀部政男: 日本と世界のプライバシー・個人情報保護論議, 2003年5月15日