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

村上　康二郎[1]

概 要

クラウド・コンピューティングの登場および普及によって，様々な法的課題が発生しているが，その中でも，個人情報保護に関する問題は，中心的な問題になるものと考えられる．クラウド・サービスを提供する事業者（本稿では，「クラウド事業者」と称する）が，ユーザに関する個人情報を取得する場合や，クラウド・サービスを利用する事業者（本稿では，「クラウド・サービス利用者」または「利用者」と称する）がユーザの個人情報を取得し，当該事業者がそれらの個人情報をクラウド事業者において保存，管理する場合などが想定されるが，このような場合には，個人情報保護に関する様々な問題が発生することになる．クラウド・コンピューティングの個人情報保護に関する課題も様々な観点からの検討が可能であるが，本稿は，クラウド・コンピューティングに対して，我が国の「個人情報の保護に関する法律」（本稿では，「個人情報保護法」と表記する）がどのように適用されるのかという問題を中心に検討するものである[2]．

1　はじめに

クラウド・コンピューティングにおけるプライバシーや個人情報保護の問題については，すでにいくつかの文献が存在するが，まとまった検討を行っているものとしては，(1) Mather et al.[2009]，(2)白石[2011]，(3)鈴木[2012]などがある[3]．

(1)の Mather et al.[2009]は，クラウドにおけるプライバシー懸念として，以下のものをあげている．①アクセス（組織が個人に対して，すべての個人情報へのアクセスを提供できるのか．情報主体がデータの削除を求めたとき，組織はクラウドにある情報を削除できるのか），②コンプライアンス（個人情報の管理にどんな法律，規制，契約が適用されるの

---

[1] 東京工科大学 教養学環 准教授

[2] なお，本稿は，2010 年度に，株式会社富士通総研の委託に基づき，林紘一郎先生が委員長として実施された「クラウド時代の法制度と情報セキュリティ」研究会の報告書のうち，筆者が執筆した部分について，加筆や修正を加えたものである．そのため，最近起こったファーストサーバ事件との関係には触れていないし，その他，最近の議論動向については十分な言及ができていない部分がある．このような不十分な論文ではあるが，林先生の学長退任記念特集号に，林先生が委員長を務められた研究会の成果を掲載させていただくことにも一定の意味があると考え，寄稿させていただいた次第である．なお，個人的には，類似のテーマについて，株式会社富士通研究所の受託研究も行った．林先生や，富士通グループの関係者の皆様に対して，この場を借りて感謝を申し上げたい．

[3] その他の文献としては，堀部[2010]，下道[2010]，吉井[2011]，近藤＝松本[2011]，クラウド・コンピューティング関連法研究会[2012a]，同[2012b]などがある．なお，クラウドにおける営業秘密の問題について論じたものとしては，夏井[2010]がある．

情報セキュリティ総合科学 第 4 号　2012 年 11 月、論文受付 2012 年 8 月、同 10 月採録

か），③ストレージ（データはどこに格納されるのか），④保持（どんな保持ポリシーでデータを管理するのか．誰が保持ポリシーを実施するのか），⑤破棄（クラウドプロバイダは，どのように情報を破棄するのか），⑥監査とモニタリング（どのようにクラウドプロバイダをモニタリングし，プライバシー要求が遵守されているという保証を与えるのか），⑦プライバシー侵害（どうすればプライバシー侵害の発生がわかるのか）である．

また，(2)の白石[2011]では，クラウド・コンピューティングに対して，我が国の個人情報保護法がどのように適用されるのかという観点から，以下の 3 つの問題を重点的に論じている．すなわち，①クラウド・コンピューティング事業者のサーバで切片化[4]された情報の個人情報該当性，②クラウド・コンピューティング上での個人データの取扱いと個人情報保護法上の責任（個人データの「第三者提供」と「委託」，クラウド・コンピューティング事業者の個人情報取扱事業者該当性），③クラウド・サービスの利用と国境を越える個人情報の移転である．

(3)の鈴木[2012]も，(2)と同様に，クラウド・コンピューティングに対して，個人情報保護法がどのように適用されるのかという観点から論じており，個人データの安全管理義務違反の問題，個人データ提供の委託該当性の問題などが論じられている．

本稿は，クラウド・コンピューティングへの我が国の個人情報保護法の適用を中心に論じるものなので，上記の文献のうち，主に(2)と(3)が関係してくる．この中で，(2)の白石[2011]は，我が国においても有数な法律事務所に所属している弁護士陣が執筆した書籍の中の 1 章であるため，法律実務に対して，大きな影響を与える可能性がある．確かに，意欲的な論文ではあるが，個人的には，疑問に感じている点も多いので，本稿では，特に，同論文に対して批判的な観点から検討を進めていくことにしたい．

以下では，まず議論の前提として，個人情報保護法制に関する基本的事項をごく簡単に整理する（2）．その上で，クラウド・コンピューティングに関する個人情報保護の問題について，白石[2011]が取り上げている問題点，すなわち，クラウド事業者が切片化した情報の個人情報該当性（3），個人データの「委託」と「第三者提供」（4），クラウド事業者の個人情報取扱事業者該当性（5），クラウド・コンピューティングと国境を越える個人情報の移転（6）について，検討を加えることにする．

2　個人情報保護法制の概要

ここでは，クラウド・コンピューティングに個人情報保護法がどのように適用されるのかという問題を検討する前提として，我が国の個人情報保護法制の概要を整理することにする．

2.1　個人情報保護関連 5 法の制定

我が国では，1988 年に「行政機関の保有する電子計算機処理に係る個人情報保護に関する法律」が制定されたが，その際は，民間部門を規制する法律は制定されなかった[5]．

[4] 「切片化」という言葉について，白石[2011]では特に定義はなされていないが，「一つのデータを細かく分割する」という意味合いで用いられているものと推測される．

[5] 我が国における個人情報保護法制定にいたる経緯については，園部編[2005]5 頁以下，岡村[2009]10 頁以下，宇賀[2009]1 頁以下，三宅＝小町谷[2003]54 頁以下など参照．

しかし，その後，主として以下の 4 つの理由から，民間部門についても法整備が必要であると認識されるようになった[6]．すなわち，①1980 年 OECD プライバシー・ガイドラインへの対応，②1995 年 EU 個人データ保護指令への対応（同指令 25 条は，加盟国から第三国への個人データの移転は，当該第三国が十分なレベルの保護を提供している場合に限定している），③情報化社会の進展により個人情報の大量漏洩事件が頻発するようになったことへの対応，④住民基本台帳ネットワークシステムの導入によって，個人情報漏洩の危機が生じる恐れがあることへの対応である．

このような認識を背景として，2003 年 5 月に，個人情報保護関連 5 法が制定された．これは以下の 5 つの法律からなる．①「個人情報の保護に関する法律」（個人情報保護法），②「行政機関の保有する個人情報の保護に関する法律」（行政機関個人情報保護法），③「独立行政法人等の保有する個人情報の保護に関する法律」（独立行政法人等個人情報保護法），④「情報公開・個人情報保護審査会設置法」（設置法），⑤「行政機関の保有する個人情報の保護に関する法律等の施行に伴う関係法律の整備等に関する法律」（整備法）．

2.2 個人情報保護法の概要

クラウド・コンピューティングを民間の企業において利用する場合には，上記の個人情報保護関連 5 法のうち，特に①の個人情報保護法が関係してくることになる．この法律は，基本理念などを定めた基本法部分と，民間部門に関する一般法部分とから構成される．まず，基本法部分では，基本理念，政府による個人情報の保護に関する施策の基本となる事項，国および地方公共団体の責務が定められている．次に，民間部門に関する一般法部分においては，個人情報取扱事業者の義務が定められている．すなわち，個人情報取扱事業者を「個人情報データベース等を事業の用に供している者」（2 条 3 号）と定義し，この個人情報取扱事業者は，その取り扱う情報の種類により，原則として，以下のような義務を負うとしている．

- 「利用目的の特定」（15 条）：
  個人情報を取り扱うに当たって，その利用の目的をできる限り特定しなければならない
- 「利用目的による制限」（16 条）：
  あらかじめ本人の同意を得ないで，特定された利用目的の達成に必要な範囲を超えて個人情報を取り扱ってはならない
- 「適正な取得」（17 条）：
  偽りその他不正な手段により個人情報を取得してはならない
- 「取得に際しての利用目的の通知」（18 条）：
  個人情報を取得した場合は，あらかじめその利用目的を公表している場合を除き，速やかに，その利用目的を本人に通知し，または公表しなければならない
- 「データ内容の正確性の確保」（19 条）：
  利用目的の達成に必要な範囲内において，個人データを正確かつ最新の内容に

[6] 岡村[2009]10 頁以下

保つよう努めなければならない

・「安全管理措置」(20 条)：
個人データの安全管理のために必要かつ適切な措置を講じなければならない

・「従業者の監督」(21 条)，「委託先の監督」(22 条)：
従業者，委託を受けた者に対する必要かつ適切な監督を行わなければならない

・「第三者提供の制限」(23 条)：
あらかじめ本人の同意を得ないで，個人データを第三者に提供してはならない

・「保有個人データに関する事項の公表」(24 条)：
保有個人データに関する事項を本人の知り得る状態に置かなければならない

・「開示」(25 条)，「訂正」(26 条)，「利用停止」(27 条)：
本人から開示の求めがあった場合，応じなければならない．また，一定の要件を満たす場合には，訂正，利用停止などの求めに応じなければならない

これらのうち，15 条から 18 条は「個人情報」(「生存する個人に関する情報であって，当該情報に含まれる氏名，生年月日，その他の記述により特定の個人を識別できるもの(他の情報と容易に照合することができ，それにより特定の個人を識別することができることとなるものを含む)」)について適用される義務である．また，19 条から 23 条は「個人データ」(「個人情報データベース等を構成する個人情報」)にのみ適用される義務である．そして，24 条から 27 条は「保有個人データ」(「個人情報取扱事業者が，開示，内容の訂正，追加又は削除，利用の停止，消去及び第三者への提供の停止を行うことのできる権限を有する個人データ(以下省略)」)にのみ適用される義務である．

これまで整理してきたことを踏まえつつ，以下では，白石[2011]が議論している課題を中心的に取り上げて検討を加えることにしたい．

3　クラウド事業者が切片化した情報の個人情報該当性

クラウド・コンピューティングでは，Google File System のような分散ファイルシステムが用いられ，これによって一つのファイルに関するデータが切片化された上で，保存されることがあるといわれている．白石[2011]113 頁以下は，個人情報を含むファイルが切片化されて異なるサーバに保存された場合には，個人情報保護法上の個人情報に該当しなくなるのではないかという問題提起を行っているが，果たしてそのように考えてよいのかが問題となる．

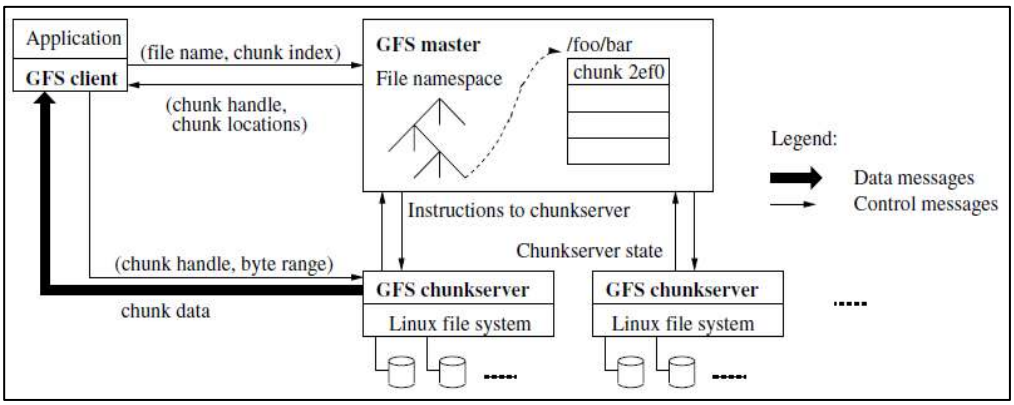
3.1　分散ファイルシステム　—Google File System を中心として—

濱野[2011]11 頁以下では，Google のシステムを例に，クラウドにおける分散処理について，説明されている．クラウド・コンピューティングを支える技術としては，仮想化技術のほかに，分散処理技術がある．この分散処理技術によって，インターネットを通じたサービスの提供が高速で行われることが可能になるということである．

前掲濱野論文によれば，Google File System(GFS)は，Google の分散処理システムを構成する一つの要素で，そのほかに，分散データベースシステムである Bigtable，分

散処理アルゴリズムである MapReduce がある．この GFS は，一つのファイルを 64M のデータの塊に分割した上で，保存するものである．このデータの塊のことをチャンク（Chunk）と称する．そして，GFS は，一つのマスタと複数のサーバ（「チャンクサーバ」と呼ばれる）から構成されている．マスタは，すべてのファイルシステムのメタデータのみを有しており，実際のデータは分割され，複数のサーバに分散して保存されることになる（図表 1 を参照）．

図表 1　Google File System のアーキテクチャ（Ghemawat et al.[2003]）



3.2　個人情報保護法における個人情報概念

上述のような分散ファイルシステムによって，ユーザの個人情報が切片化された場合に，当該情報が個人情報保護法上の個人情報に該当するのかが問題となる．前提として，まず，個人情報保護法上の個人情報概念について整理しておくことにする．

個人情報保護法 2 条 1 項は，個人情報を以下のように定義している．すなわち，「生存する個人に関する情報であって，当該情報に含まれる氏名，生年月日その他の記述等により特定の個人を識別することができるもの（他の情報と容易に照合することができ，それにより特定の個人を識別することができることとなるものを含む．）をいう」というものである．

この条文の定義を分析すると，個人情報に該当するための要件として，次の 3 つを抽出することができる．すなわち，①生存性（生存する個人に関する情報であること），②個人識別性（特定の個人を識別することができるものであること），③容易照合性（他の情報と容易に照合することによって特定の個人を識別することができるものであること）である[7]．もっとも，この 3 つを常に満たしている必要はなく，①と②を満たしていれば，それだけで個人情報となるが，②を満たしていなくとも，③が満たされればそれは個人情報に該当することになる．

[7] 文献によっては，「個人識別性」は，「識別可能性」と表記されることがある．また，「容易照合性」は「照合容易性」と表記されることがある．これらは表現が異なるだけで内容的には同じものをさしている．

クラウド事業者によって切片化されたデータについては，上記の 3 つのうち，特に②の個人識別性と③の容易照合性が満たされるのかが問題となる．

3.3 クラウド事業者によって切片化されたデータに関する議論

それでは，クラウド事業者が，ユーザの個人情報を Google File System のような分散ファイルシステムを用いて保存している場合，それは個人情報に該当することになるのであろうか．

この問題について，白石[2011]は，識別可能性，照合容易性のいずれも否定し，結果的に個人情報該当性を否定する見解を主張している．まず，識別可能性については，次のような「モナリザの絵画」の例をあげて議論を展開している．すなわち，「モナリザの絵画」のジグソーパズルがあり，各ピースに IC チップが埋め込まれているため，IC リーダを使用すると全体として「モナリザの絵画」を構成することが分かるが，IC リーダを使用しないと分からないというケースを想定する．その上で，各ピースに接しただけでは，それが「モナリザの絵画」の一部であることを判別できる者はいないであろうから，個々のピースに「モナリザの絵画」としての識別可能性はないとする．クラウド事業者によって切片化されたデータもこれと同じで，切片化されたデータには，個人情報としての識別可能性はないとするのである．

次に，照合容易性については，まず，クラウド事業者が，各切片がいかなる個人情報の一部を構成するものなのかを判別することはできないということを前提とする．そして，切片化されたデータがいかなる個人情報を構成するのかを判別するためには，切片化されたデータのすべてを照合することが必要になるが，「どのサーバのどこに保存されているかわからない，一つの個人情報を構成しているほかのデータの切片すべてを照合することは容易ではなく，『容易』との要件が欠ける」と主張する．

これらの分析を踏まえた上で，クラウド・サービス利用者 A が，クラウド事業者 B に顧客の個人情報を提供する場合について，次のように論じる．A にとって識別性があるが，B や通常人にとって識別性のない情報を，A が B に提供する場合には，個人の権利利益の侵害のおそれが発生しないため，第三者提供の規制はかからないという見解が存在する[8]．この見解を基礎としつつ，ID・パスワードがクラウド・サービス利用者 A によって管理されており，クラウド事業者 B がそれを知らない場合には，クラウド事業者 B にとって，「切片化されたデータをすべて集めて意味を持った一つのまとまりのある情報として読み出すことは容易ではない」と主張する．結局，この場合，クラウド・サービス利用者 A にとっては，識別可能性があるが，B にとっては識別可能性がないため，第三者提供の規制はかからないと主張するのである．

3.4 クラウド事業者によって切片化されたデータに関する検討

上記の白石[2011]の見解は，クラウド・コンピューティングにおける分散ファイルシステムの仕組みに着目した分析として注目されるものであるが，様々な問題点ないし疑問点が存在するように思われる．

[8] 岡村[2009]76 頁など

法的な問題に入る前に，はじめに，技術的な問題点について指摘しておきたい．というのは，検討の前提となるクラウド・コンピューティングにおける分散ファイルシステムという技術に関する理解について，問題があるように感じられるからである．まず，クラウド事業者のすべてが，Google の GFS のような分散ファイルシステムを利用しているわけではない．分散ファイルシステムを用いていない場合には，そもそも上述のような議論は，当てはまらないことになる．また，特に問題になるのは，Google の GFS のような分散ファイルシステムと，セキュリティ技術の一つである「秘密分散技術」ないし「秘密分散法」[9]は異なるものであるにもかかわらず，白石[2011]では，この二つが混同されて議論されてしまっている点である．前者の分散ファイルシステムは，データの秘匿化を目的としたものではなく，大量のデータを効率よく処理することを目的としたものに過ぎない．また，一部のサーバないしマシンが故障しても大丈夫なように，複数のサーバに複製を保存するものであり，機密性よりも可用性を重視したものになっている[10]．これに対して，後者の秘密分散技術は，データの秘匿化を目的としたセキュリティ技術の一つであって，両者は区別する必要がある．個人情報について秘密分散技術を用いた場合の法的評価については，別途，検討の余地があるが[11]，単に GFS のような分散ファイルシステムを用いているだけの場合に，単純に個人情報該当性を否定してよいのかについては，より慎重な検討が必要であると考えられる．このような技術的な理解を前提に，以下，法的問題に関する疑問点について見ていくことにする．

第一に，白石[2011]が，識別可能性について，「モナリザの絵画」を例に検討している点は，興味深いものではあるが，切片化されたデータが常に識別可能性を有しないのかについては，疑問がないわけではない．確かに，ユーザの個人情報がクラウド事業者のサーバにおいて，切片化された場合，個々の切片化されたデータだけを見ても，それがどのような個人情報の一部を構成するのかは分からない場合が多いであろう．しかし，例えば，個々の切片化されたデータに，氏名その他の特定個人を識別可能な情報がメタデータなどの形式で付されている場合には，個々の切片化されたデータも個人識別性を有することになるものと解される．したがって，常に切片化されたデータが識別可能性を有しないと解するのは適切ではないものと考えられる．

第二に，白石[2011]では，切片化されたデータがどの事業者との関係で個人情報該当性を有しないと主張しているのか，記述があいまいで必ずしも明確ではないところが存在する．少なくとも，ユーザの個人情報をクラウド・サービス利用者 A が取得し，利用している場合，クラウド事業者 B によって当該データが切片化されたとしても，A にとっては，当該情報は個人情報であることは否定できないところである．この点については，一応，認識されているようであるが，ある情報が個人情報に該当するかどうかについては，個人情報取扱事業者ごとに相対的に判断する必要があるというのが，一般的な考え方であり[12]，どの事業者との関係で個人情報該当性を検討するのかを常に意識することが重要であると考

[9] 秘密分散技術ないし秘密分散法については，差し当たり，山本[2004]や藤村ほか[2005]などを参照．このような技術は，「電子割符」と称されることもある．

[10] Google File System については，加藤[2011]86 頁以下などを参照．

[11] 個人情報を秘密分散技術によって分割した場合の分割片が個人情報に該当するかということ自体，暗号化された情報の個人情報該当性に関する論点との関係も踏まえて，慎重な検討が必要な問題である．通常の暗号技術と秘密分散技術とは異なるということが指摘されており，その点をどのように法的に評価するかが問題となるが，ここでは深入りしないことにしたい．秘密分散技術によって細分化された分割片は，個人情報に該当しないとするものとして，NRI セキュアテクノロジーズ[2010]170 頁がある．なお，藤村ほか[2005]も参照．

[12] 岡村[2009]75 頁以下，鈴木[2004]92 頁以下など

えられる[13].

第三に，白石[2011]は，クラウド事業者 B が，個人情報を切片化した後のデータに焦点を当てて議論しているが，少なくとも，クラウド・サービス利用者Aから，クラウド事業者Bに，個人情報が提供される際には，当該情報はまだ切片化されていないと考えられるため，その時点では個人情報であるということをどのように評価するのかという問題がある．この点については，第三者提供を規制している個人情報保護法 23 条を素直に文理解釈すれば，むしろ 23 条の適用ありということになるのではないだろうか．白石[2011]は，個人の権利利益の侵害のおそれがないとして，第三者提供の規制を否定するのであるが，それは一種の縮小解釈であり，そのような縮小解釈が認められるのかどうかについては，慎重な検討が必要になるものと考えられる．

第四に，最も大きな問題として，クラウド事業者 B が個人情報を切片化した場合に，常に容易照合性がないといえるのかという問題がある．この点，白石[2011]は，当該データが切片化され，異なるサーバに分散して格納される点を強調している．しかし，そもそも，容易照合性とは，「通常の業務における一般的な方法で，個人を識別する他の情報との照合が可能な状態である」とされており，容易照合性がないのは，「システムが異なる等の事情により技術的に照合が困難」なような場合である[14]．したがって，いかに切片化され，それぞれが異なるサーバに保管されていても，当該事業者の通常の業務の範囲内において，システム上それらを照合することが可能な状態になっていれば，容易照合性はありということになるものと考えられる．確かに，切片化されたデータを照合して個人情報として読み出すための ID・パスワードを利用者 A のみが有しており，クラウド事業者 B が有していない場合もありうるであろう．しかし，クラウド事業者が，切片化されたデータが，もとの個人情報と一致しており，完全性，正確性を担保しているかどうかを確認する必要がある場合もあるものと想定され，そのような場合には，クラウド事業者も，システム上，切片化されたデータを照合して個人情報として読み出すことが可能な状態にしておく必要がある．この問題については，クラウド事業者がどのような形でデータを切片化しているかなどによって左右されるところであり，常に，クラウド事業者によって切片化されたデータに個人情報該当性が認められないとすることは適切ではないように思われる．

4　個人データの「委託」と「第三者提供」

クラウド・コンピューティングにおいては，個人情報取扱事業者であるクラウド・サービス利用者が，ユーザに関する個人データをクラウド事業者において管理する場合に，それが，個人情報保護法上の「委託」に該当するのか，それとも「第三者提供」に該当するのかが問題となる．クラウドの問題が取り上げられるようになった初期のころに，様々な研究会が報告書を公表したが，その中には，クラウド・サービス利用者が，個人データをクラウド事業者において管理する行為を当然に，「委託」に該当することを前提とした記述をしているものもあった[15]．これに対して，総務省の「スマート・クラウド研究会」の報告書は，

[13] 鈴木[2012]144 頁は，白石論文に対して，以下のような批判を加えている．「個人情報該当性判断において，特定個人の識別性や容易照合性を誰が判断するのかという論点について，本人を基準とするのか，一般人を基準とするのか，提供事業者の他に受領事業者の識別性の有無も影響するのか，個人の権利利益の侵害のおそれの有無も影響するのか否か，判断の悩ましさは十分に伝わってくるが，必ずしも理由付けとして明快ではない」．

[14] 園部編[2005]49 頁．

[15] 情報処理推進機構[2010]106 頁

上記のような行為が「委託」に該当するのかどうかについて検討が必要であると指摘している[16]．そこで，以下ではこの問題点について検討を加えることにしたい．

4.1 個人情報保護法における「委託」と「第三者提供」

まず，議論の前提として，個人情報保護法において，「委託」および「第三者提供」の規律がどうなっているのか，またどのような場合に「委託」になり，どのような場合に「第三者提供」になるのかといった事項について整理することにする．

委託について，個人情報保護法 22 条は，次のように規定している．すなわち，「個人情報取扱事業者は，個人データの取扱いの全部又は一部を委託する場合は，その取扱いを委託された個人データの安全管理が図られるよう，委託を受けた者に対する必要かつ適切な監督を行わなければならない」というものである．

また，第三者提供については，個人情報保護法 23 条によれば，原則として，あらかじめ本人の同意を得ることが必要とされている．すなわち，同条 1 項は，「個人情報取扱事業者は，次に掲げる場合を除くほか，あらかじめ本人の同意を得ないで，個人データを第三者に提供してはならない」とする．

それでは，どのような場合が「委託」になり，どのような場合が「第三者提供」になるのであろうか．この点については，これまで十分に議論されてこなかった部分もあるように思われるが，どのような場合が委託に該当するのかについては，一応，以下のような説明がなされている．すなわち，「『委託』とは，委任契約，請負契約といった契約の形態・種類を問わず，個人情報取扱事業者が他の者に個人データの取扱いの全部又は一部を行うよう依頼する契約の一切を含むものである．具体的には，個人情報取扱事業者が外部の情報処理会社等に対して個人データの入力，編集，出力等の処理を行うことを依頼すること等が想定される」[17]ということである．

4.2 クラウド・サービスの利用の「委託」該当性に関する検討

クラウド・サービス利用者が，クラウド事業者に顧客の個人データを預ける場合に，これが「委託」に該当するのか，「第三者提供」に該当するのかが問題となるが，白石[2011]120 頁以下は，以下のような立場に立っている．すなわち，クラウド・サービス利用者が保管する個人データについて，クラウド事業者が「独自の利用目的」を有しているか否かを基準とし，「独自の利用目的」を有していない場合には，「委託」に該当するが，「独自の利用目的」を有している場合には，「第三者提供」に該当すると解するのである．そして，クラウド事業者は，独自の利用目的を有していないことが多いとし，結果的に，多くの場合は委託に該当するという立場に立っている[18]．

このような「委託」と「第三者提供」の区別の仕方については，一つの説明の仕方としてありうるものであると考えられる．あるいは，見方を少し変えれば，次のようないい方もできるかもしれない．すなわち，委託の場合には，委託元が契約によって定めた目的につ

16 総務省[2010a]25 頁
17 園部編[2005]142 頁
18 同旨のものとして，クラウド・コンピューティング関連法研究会[2012b]69 頁がある．同論文は，「一般に，クラウド事業者は，利用者が保管する個人データについて独自の利用目的を有しないと考えられるので，利用者は，当該利用者が保管する個人データの取扱いをクラウド事業者に対して，利用者の利用目的の達成に必要な範囲内で委託したものと位置づけられ，本人の同意を必要としない個人情報保護法 23 条 4 項 1 号の『委託』に該当すると解される」としている．

いてのみ，委託先は個人データを取扱うことができるのに対して，第三者提供の場合には，契約によって定められた目的とは関係なく，独自の利用目的のために提供先は個人データを利用することができるということである．クラウド・サービスについて，現在，どのようなタイプのサービスが普及しているのかは不明なところもあるが，従来の一般的な説明を前提とすれば，クラウド・コンピューティングの場合は，「委託」に該当することが多いのではないかと推測される[19]．

4.3 問題点に関する検討

このように，クラウド・サービスの利用は「委託」に該当することが多いとして，ここからさらに新たな問題が発生することになる．委託に該当する場合，委託元であるクラウド・サービス利用者は，委託先であるクラウド事業者に対して，「必要かつ適切な監督をしなければならない」ことになる（個人情報保護法 22 条）．「必要かつ適切な監督」の内容としては，各省庁から出されているガイドラインを基礎に，①委託先を適切に選定し，②委託契約に必要・適切な条項を定めた上，③委託先における遵守状況・取扱状況を確認することであるとされている[20]．

しかし，このような監督が現実に可能なのかということが問題となる．この点については，高度で複雑なクラウド・サービスについては，サービス利用者はクラウド事業者を適切に監督するだけの能力やリソースを持っていないのではないかという指摘がなされている[21]．また，クラウド・サービス利用者が，中小企業であり，クラウド事業者が大企業である場合も多く存在するのではないかと考えられるが，このような場合には，クラウド・サービス利用者が，クラウド事業者を適切に監督することは，実際上難しいところがあるように思われる．これらの問題点は，もともと個人情報保護法 22 条に内在する問題ともいえるが，それがクラウドの場合には増幅されるところがあるといえるであろう．つまり，クラウドの場合には，サービスがより高度で複雑なものになるため，委託先における取扱状況を確認することはより困難になるし，中小企業が大企業に対して委託を行うことが多くなるため，実効的な監督を行うことがより難しくなるということである．

このような問題点を解決するために，白石[2011]122 頁は，次のような見解を主張している．すなわち，クラウド事業者が個人データを切片化して保管する場合には，当該データは，個人識別性（ひいては個人情報該当性）を失うので，「個人データの取扱いの全部又は一部を委託する場合」という要件を欠くことになり，個人情報保護法 22 条による監督責任は発生しないというものである．しかし，クラウド事業者がデータを切片化して保管した場合に，個人情報該当性を否定する見解については，様々な疑問があり，慎重な検討が必要であることは，前述したとおりである．また，クラウド事業者が分散ファイルシステムを利用してデータを切片化していない場合には，このような議論はもともと当てはまらないという限界も存在するところである．

それでは，この問題をどのように解決すればよいかということであるが，この点について

[19] この点について，鈴木[2012]148 頁は，「クラウドサービスは，従前の IT サービスに比較し，複雑なシステム構成をなしているとはいえ，基本は情報処理の委託（IT アウトソーシング・サービスの一つ）である」としつつ，「委託した個人データの一部について，契約終了後もユーザに返還されずベンダにとどまることがあるならば，当該データに着目して，そこに第三者提供を観念する余地がある」としている．
[20] 岡村[2009]232 頁
[21] 白石[2011]121 頁以下，クラウド・コンピューティング関連法研究会[2012b]69 頁など

は，いくつかの解決策が提示されている．まず，「委託先における個人データ取扱状況の把握となると，現実的にはベンダのデータセンターに確認に出向くということはできないものが大半であろう」という認識を前提として，「ヒアリング項目を書面で送り回答を求めるなどの代替的対応を解釈上容認するほかない」という提案をする見解が存在する[22]．また，「利用者が個人データの管理状況をモニタリングしやすいように，クラウド事業者に定期的に監査レポートを提出する義務を負わせること等により，クラウド事業者におけるデータの取扱いを監督しやすくし，クラウド事業者の安全管理対策を向上させ，もって，利用者の個人情報を監督している状況を作り出すことによって，その義務を履行しているものと考えるべきである」とする見解も主張されている[23]．クラウド・サービスにおける委託先の監督に関する問題については，これらの見解を基礎にしながら，技術的な観点も含めて，対応策を検討していくのが妥当ではないかと考えられる．

5　クラウド事業者の個人情報取扱事業者該当性

クラウド・コンピューティングにおいては，クラウド事業者が，個人情報保護法上の個人情報取扱事業者に該当するのかということが問題となる．

個人情報取扱事業者とは，「個人情報データベース等を事業の用に供している者」をいう（個人情報保護法 2 条 3 項）．そして，個人情報保護法 2 条 3 項 5 号および施行令 2 条によって，その事業の用に供する個人情報データベース等を構成する個人情報によって識別される特定の個人の数の合計が過去 6 月以内のいずれの日においても 5000 を超えない者は，個人情報取扱事業者に該当しないものとされている．以下，クラウド事業者が，このような個人情報取扱事業者に該当するのかどうかについて検討していくことにする．

5.1　クラウド事業者の個人情報取扱事業者該当性に関する議論

この問題点について，白石[2011]124 頁以下は，クラウド事業者が利用者の個人データについて独自の利用目的を有しない場合には，クラウド事業者は，個人情報取扱事業者に該当しないという見解を主張している．その理由としては，以下の諸点があげられている．

①第一に，「個人情報の保護に関する法律についての経済産業分野を対象とするガイドライン」[24]（以下では，「経済産業分野ガイドライン」と称する）では，倉庫業者やデータセンターが，個人情報が含まれていることを認識しないまま預かっている個人情報について，個人情報取扱事業者該当性を判断する際の数に算入しないとされていることなどを指摘する．そして，クラウド事業者も倉庫業者やデータセンターと同様であるため，独自の利用目的を有しないクラウド事業者の個人情報取扱事業者該当性を否定すべきであるとする．②第二に，クラウド・サービス利用者の個人情報データベースのうちから，特定のデータを取り出して，クラウド上で利用する場合，クラウド事業者は，単体のデータを見ても利用者の下で個人情報データベースを構成していたかどうか判別できないとする．③第三に，ク

[22] 鈴木[2012]150 頁
[23] クラウド・コンピューティング関連法研究会[2012b]69 頁
[24] 経済産業省[2009]6 頁

ラウド・サービス利用者が，個人情報データベースをクラウド事業者が提供するサーバなどを利用して構築した場合であっても，クラウド事業者は，利用者が構築した個人情報データベースにアクセスできず，自己の事業に役立たせているわけでもなく，利用者が構築した個人情報データベースの内容を関知することなく保管しているだけなので，「事業の用に供している」とはいえないとする．

注目される見解ではあるが，この見解については，表現がやや誇張されているところもあり，そのため誤解を招きやすい部分があるように思われる．上記の根拠のうち，①と③は似たようなことを述べているが，議論を正確に行うために，経済産業分野ガイドラインの記述を記載することにする．同ガイドラインの 6 頁には，「事業の用に供しないため特定の個人の数に算入しない事例」として，次のものがあげられている．すなわち，「倉庫業者，データセンター（ハウジング，ホスティング）等の事業において，当該情報が個人情報に該当するかどうかを認識することなく預かっている場合に，その情報中に含まれる個人情報」というものである．そして，これには但書きがあり，「ただし，委託元の指示等によって個人情報を含む情報と認識できる場合は算入する」と記載されている．ここで重要なことは，特定の個人の数に算入されないのは，当該事業者が，当該情報に個人情報が含まれているという認識がない場合に限られるということである．ところが，白石[2011]では，これが，いつのまにか「独自の利用目的を有しない場合」というあいまいな基準に置き換えられており，さらには，およそクラウド事業者は，「内容を関知することなく保管等しているだけ」であるというように一般化されてしまっている．これは，経済産業分野ガイドラインを不正確に拡張してしまっているところがあるように思われる．クラウド事業者が，独自の利用目的を有しない場合であっても，委託元からの指示などによって，当該情報に個人情報が含まれていることを認識している場合も十分存在するものと考えられる．そのような場合には，当該クラウド事業者は個人情報取扱事業者に該当すると解するのが妥当である．したがって，独自の利用目的を有しないクラウド事業者がすべて個人情報取扱事業者に該当しないとするのは相当ではない．

なお，上記の根拠のうち②については，対象となる場面を絞り込みすぎているように思われる．ここでは，クラウド・サービス利用者の個人情報データベースのうちの一部の情報をクラウド事業者が保管する場合が念頭におかれているが，実際には，利用者の個人情報データベース全体をクラウド事業者において保管する場合もかなりあるものと推測される．したがって，②において指摘されていることを，一般化することは妥当ではないものと考えられる．

5.2 IaaS 事業者・PaaS 事業者の個人情報取扱事業者該当性

また，白石[2011]127 頁以下は，インフラストラクチャを提供する IaaS 事業者およびプラットフォームを提供する PaaS 事業者は，個人情報取扱事業者に該当しないという見解を唱えている[25]．その根拠としては，主に以下の点があげられている．

まず，既存の社会的インフラを提供している事業者として，郵便会社，鉄道会社，運

[25] 白石[2011]は，IaaS と PaaS について厳密な定義を行っていないが，同じ書籍に掲載されている濱野[2011]6 頁以下の定義を前提にしているものと考えられる．そこでは，IaaS は，「サーバの CPU，ストレージ等のインフラストラクチャをインターネット経由で提供するサービス」であり，PaaS は，「アプリケーションを稼動させるプラットフォーム機能をインターネット経由で提供するサービス」であるとされている．なお，SaaS については，「アプリケーションソフトウェアの機能をインターネット経由で提供するサービス」であるとされている．

送会社，電力会社，電気通信事業者などがあるが，これらの既存インフラ事業者を通して運ばれる個人情報について，個人情報保護法に基づく保護を期待する者はいないということを指摘する．その上で，クラウド事業者のうち，IaaS 事業者や PaaS 事業者については，既存インフラ事業者と同様にインフラを提供しているだけで，クラウド・サービス利用者が保管する個人データについて独自の利用目的を有しない場合がほとんどであるとする．そのため，IaaS 事業者および PaaS 事業者は，既存インフラ事業者と同様に取り扱われるべきであるとするのである．

このような見解は注目されるものであるが，一定の限界を有するものと考えられる．確かに，IaaS 事業者や，PaaS 事業者が，既存の社会インフラ事業者と同じように，そこで取り扱っている情報の内容に全く関与しないものであるならば，それらは個人情報取扱事業者に該当しないという解釈もありうるように思われる．しかし，そのような IaaS 事業者，PaaS 事業者と，SaaS 事業者とが釈然と区別することができるのかということが問題となる．クラウド・サービスを提供している代表的な企業として，Google，Salesforce.com，マイクロソフトなどがあるが，これらはいずれも，SaaS と PaaS の両方のクラウド・サービスを提供している[26]．たとえば，Google であれば，SaaS として，Gmail，Google サイト，Google カレンダー，Google ドキュメントを利用することができる Google Apps を提供し，また PaaS としては Google App Engine を提供している．また，日本の代表的なクラウド事業者としては，たとえば，富士通があるが，同社は，SaaS，PaaS，IaaS のいずれのサービスも提供している[27]．このように，IaaS，PaaS だけではなく，SaaS も提供している事業者については，白石[2011]があげているような根拠に基づいて，個人情報取扱事業者該当性を否定することはできないものと考えられる．

もっとも，IaaS，PaaS だけを提供しているクラウド事業者も存在するようであり，そのような事業者については，上記のような議論が当てはまる可能性はある．また，一定の範囲のクラウド事業者が社会インフラ性を有するという指摘は興味深いものがあり，既存社会インフラと比較した場合の法的位置づけや，社会インフラ性に基づく法規制の要否などについては，本稿では立ち入ることができないが，今後，議論をしていく必要があるものと考えられる．

6　クラウド・コンピューティングと国境を越える個人情報の移転

クラウド・コンピューティングにおいては，ユーザの個人情報が海外のクラウド事業者やデータセンターに保管されたり，ユーザの個人情報に関するデータベースをクラウド・サービス利用者が作成し，当該データベースを海外のクラウド事業者やデータセンターに保管したりするような場合が想定される．これによって，個人情報の越境流通が生じることになり，以下のような問題が発生する．

クラウド・サービスが複数の法域にまたがる場合，各法域の個人情報保護に関する法規が適用されることになるが，それらの適用関係が問題となる．EU やアメリカを含めて，世界の国々が定めている個人情報保護に関する法制度は異なるため，それが越境流通

[26] 代表的なクラウド事業者のサービス内容については，日経 BP 社出版局編[2009]75 頁以下，加藤[2011]97 頁以下など参照．
[27] 〈http://jp.fujitsu.com/solutions/cloud/services/〉

の妨げになる可能性がある．場合によっては，個人情報が海外のデータセンターに保管された場合，当該国の法律によって開示を求められたり，また日本に持ち帰れなくなったりする恐れがあるという指摘もなされている[28]．このような個人情報の越境流通において特に大きな問題となるのは，EU 個人データ保護指令が，個人データの第三国移転を制限しているということである．そのため，この指令にどのように対応するのかが多くの国々にとって重大な課題になっている．他方で，日本の個人情報保護法には，個人情報の海外移転を制限する規定が存在しないが，個人情報保護法制を改正して海外移転を制限するのかということも立法論的な課題になりうるものと考えられる．

これらの越境流通に関わる課題は，別にクラウドによってはじめて生じる問題という訳ではなく，従来から存在していたものであるが，クラウドでは，個人情報の越境流通はより頻繁に，また無意識的に生じるため，問題がより深刻になるものと考えられる．

ここでは，上記の課題のすべてについて検討することは難しいため，EU 個人データ保護指令とそれに対するアメリカの対応などを中心に見ていくことにしたい．

6.1 EU 個人データ保護指令と第三国移転の制限

第三国移転の制限に入る前に，EU の個人データ保護指令の概要について簡単に見ておくことにする．諸外国の個人情報保護法制の中でも，EU 諸国は高いレベルで個人データを保護している．EU では，「個人データの処理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」（本稿では，「EU 個人データ保護指令」と表記する）[29]が重要な意味を持っている．この EU 個人データ保護指令は，公的部門と民間部門の両方を対象としている．特徴としては，個人データの収集，記録，蓄積，利用，頒布，削除などの処理を行うことについて，原則としてデータ主体の同意を要求していること（7 条），センシティブデータについては，特に厳格な保護を与えており，原則として処理を禁止していること（8 条），管理者は自動処理作業または一連の作業を実施する場合には，事前に監督機関に通知しなければならないとしていること（18 条），などをあげることができる．

そして，クラウドによる個人情報の越境流通にとって大きな問題となるのが，EU 個人データ保護指令 25 条である．同条は，次のように規定している．すなわち，「加盟国は，処理過程にある個人データ又は移転後処理することを目的とする個人データの第三国への移転は，この指令の他の規定に従って採択されたその国の規定の遵守を損なうことなく，当該第三国が十分なレベルの保護を確保している場合に限って行うことができる」というものである．つまり，個人情報について十分なレベルの保護を行っていない第三国に対しては，原則として，EU 加盟国から個人データを出してはいけないということである[30]．

また，この EU 個人データ保護指令については，2012 年 1 月 25 日に，改正案が公表されている．それが，「個人データの取扱いに係る個人の保護と当該データの自由な移動に関する欧州議会及び理事会の規則（一般データ保護規則）の提案」（本稿では，

[28] 総務省[2010b]9 頁など．白石[2011]139 頁以下も参照．
[29] 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
[30] クラウド・コンピューティングと EU 個人データ保護指令の関係については，新保[2012]417 頁以下を参照．

「EU 個人データ保護規則提案」と表記する)[31]である．全体的には，個人データの保護をより厳格にする内容のものになっている[32]．第三国移転の制限についても，基本的に，個人データ保護指令から引き継がれているが（40 条以下），さらに，違反に対する制裁が強化されている．すなわち，故意または過失によって，第三国移転の制限に関する規定に違反した場合は，最大で 100 万ユーロまたは全世界の年間売上高の最大 2%までの制裁金が科されるものとしている（79 条 6 項(1)）．

6.2 アメリカの個人情報保護制度とセーフハーバー協定

それでは，アメリカは，上記の EU 個人データ保護指令 25 条における十分性の基準を満たしているのであろうか．アメリカには，今のところ，公的部門と民間部門の両方を包括的に規制する連邦レベルの個人情報保護法は存在しない[33]．公的部門については，1974 年にプライバシー法が成立しているが，民間部門については，包括法は存在せず，基本的には自主規制に委ねられている．そして，民間部門については，特定の分野ごとに個別法が制定されている．このように，アメリカの個人情報保護制度は，EU ほど個人情報を厳格に保護していない．

そこで，問題となるのは，EU 個人データ保護指令 25 条との関係である．アメリカでは民間部門を包括的に規制する法律が存在していないため，指令 25 条の十分なレベルの保護に達していないということになり，EU 加盟国からの個人データの移転について障害が生じてしまうことになる．そこで，アメリカは，EU と協議を行い，2000 年に，セーフハーバー協定を締結するにいたった[34]．これは，一定の要件を満たしている企業，組織については，セーフハーバーという安全な港の中にあるものとして EU 加盟国から個人データの移転を受けられることにしたものである．

6.3 日本における対応

EU 個人データ保護指令 25 条に対して，日本としてどのように対応していくのかという問題は，クラウドの問題を超えて，越境流通全般に関わる重大な問題であり，軽々に論じられるものではない[35]．ここでは，以下の点を指摘するにとどめたい．同指令 25 条に対応するための方法としては，いくつかのものが考えられる．①我が国の個人情報保護法制を大幅に改正し，EU 個人データ保護指令の十分性の基準を満たすものにする，②我が国もアメリカと同じようなセーフハーバー協定を EU と締結する，③EU 個人データ保護指令 25 条の例外として認められている「標準契約条項」や「拘束的企業準則」（Binding Corporate Rules: BCR）を活用するなどである[36]．①については，EU 指令に対応するために必要であるとして積極に解する立場と，個人情報保護法制が厳格になりすぎ，我

[31] 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)
[32] EU 個人データ保護規則提案については，石井[2012]，クラウド・コンピューティング関連法研究会[2012b]71 頁以下など参照．
[33] アメリカの個人情報保護制度については，新保[2000]308 頁以下，岡村＝新保[2002]121 頁以下，石井[2008]419 頁以下など参照．
[34] セーフハーバー協定については，新保[2001]，岡村＝新保[2002]151 頁以下など参照．
[35] この問題については，堀部[2010b]1 頁以下など参照．
[36] 標準契約条項，BCR については，「国際移転における企業の個人データ保護措置調査報告書」（2010）〈http://www.caa.go.jp/seikatsu/kojin/H21report1a.pdf〉など参照．

が国の実態に合わないとして消極に解する立場とがありうるところであり，現状を打開するのは必ずしも容易ではないところがある．②については，一般的には，セーフハーバー協定は，アメリカの強い政治力があってはじめてなしえたものであるため，日本において実現することは難しいと考えられているようであるが，検討の余地はあるように思われる．いずれにせよ，①，②の実現は早急には難しいため，当面の実務的な処理としては，③を検討することが必要になっているものと考えられる．もっとも，クラウドとの関係では，BCR は，企業グループ内における個人データの利用を想定したものであり，クラウド利用者とクラウド事業者のように企業グループ外に個人データを移転する場合には利用することができないため，クラウドの場合は，標準契約条項の利用を検討するべきであるという指摘がなされている[37]．

6.4 アメリカの愛国者法（Patriot Act）

最後に，クラウドとの関係で，アメリカの愛国者法（Patriot Act）[38]がよく取り上げられるため，この点について簡単に言及しておくことにする．この愛国者法については，これまで，同法 213 条が，捜査官は令状の通知なく家宅などを捜索できると規定しているため，これによって事前の通知なくサーバが差し押さえられる可能性があるなどの指摘がなされてきた[39]．また，同法に基づいて実際に発生した事件として，アメリカのテキサス州ダラスにおいて，コア IP ネットワークスという企業のデータセンターのサーバが FBI によって押収され，約 50 社の顧客が自社のデータにアクセスできなくなった事件があげられてきた[40]．しかし，これに対しては，愛国者法によって，アメリカに所在するサーバが差し押さえられるリスクが高まったとはいえないし，コア IP ネットワーク社の事件についても，愛国者法に基づく事件なのかは必ずしも明らかではないといった，反論がなされるようになっている[41]．

この点についてどう考えるかであるが，まず，愛国者法 213 条の条文を見ると，次のように規定している．「裁判所が，予め通知することが捜査に対して悪い影響を与えると認める場合には，捜査官は，裁判所命令又は令状の執行を直ちに通知することなく被疑者の財産等について捜査を行うことができる．……また，個人は，捜査が行われてから『合理的な期間内』に通知を受けなければならない」[42]．したがって，令状の通知が全く不要としているわけではない点には注意する必要がある．捜査に悪影響を与える場合は事前に通知しなくともよいが，それでも合理的な期間内に通知しなければならないということである．また，アメリカと我が国のリスクの比較であるが，我が国では，一般的に，捜査差押のための令状は，原則として事前に通知しなければならず，実効性確保のために例外的に認められる場合でも，同時または直後の通知でなければならないと解されている[43]．そのため，我が国よりもアメリカの愛国者法の方が，令状の通知が直後ではなく，合理的期間内であればよいとされている点で，若干リスクが高いところがあり，愛国者法のリス

37 クラウド・コンピューティング関連法研究会[2012b]71 頁
38 Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act of 2001
39 経済産業省[2010]31 頁，近藤＝松本[2011]118 頁など
40 経済産業省[2010]31 頁，近藤＝松本[2011]119 頁，北川[2009]など
41 クラウド・コンピューティング関連法研究会[2012a]12 頁以下
42 訳文は，平野ほか[2002]18 頁以下による．
43 河上ほか編[2010]386 頁，田口[2009]86 頁，田宮[1996]106 頁など

クが高くないということを強調するような論調にはやや疑問が残るところである.

なお，アメリカの愛国者法との関係で，カナダのブリティッシュコロンビア州やノバスコシア州などは，政府のデータがアメリカにあるプロバイダによって格納，処理されることを禁止しているとの指摘もなされている[44].

7　おわりに

ここまで，クラウド・コンピューティングが生じさせる個人情報保護の課題について，白石[2011]が取り上げている論点を中心に検討を加えてきた．しかし，クラウド・コンピューティングによって生じる個人情報保護に関する課題は，これに尽きるものではない．最近発生したファーストサーバ事件もこの点に関係する部分があるし[45]，今後，さらに様々な課題が発生する可能性もあるものと考えられる.

なお，クラウド・コンピューティングは，利便性の向上や経費の削減など様々なメリットを有するものであって，今後もさらなる技術開発や普及が期待されるものである．しかし，はじめから，クラウドへの個人情報保護法の適用を否定しようという偏見や先入観を持って検討を行うことは適切ではないように思われる．クラウドが生じさせる個人情報保護の課題から逃げるのではなく，正面から問題を把握し，正確な議論を行うことが，むしろクラウドの発展，普及につながるのではないかと考えられる.

参考文献

[1] Tim Mather et al.[2009], Cloud Security and Privacy, p.145. 同書の翻訳として, Tim Mather ほか[2010]（下道高志監訳，笹井崇司訳）『クラウドセキュリティ＆プライバシー』（オライリージャパン）がある.
[2] 白石弘美[2011]「クラウド・コンピューティングと個人情報保護」寺本振透編集代表・西村あさひ法律事務所『クラウド時代の法律実務』（商事法務）111 頁
[3] 鈴木正朝[2012]「個人情報保護法制とクラウド」岡村久道編『クラウドコンピューティングの法律』（民事法研究会）109 頁
[4] 堀部政男[2010a]「クラウド・コンピューティング社会の進展とプライバシー・個人情報保護の論点」月報司法書士 457 号 2 頁
[5] 下道高志[2010]「クラウドコンピューティングの現状と欧米におけるプライバシーへの取組み」法とコンピュータ 28 号 119 頁
[6] 吉井和明[2011]「クラウド・サービスにおける法的リスク分析―利用者の視点から」情報ネットワーク・ローレビュー10 巻 159 頁
[7] 近藤浩＝松本慶[2011]『クラウドと法』（金融財政事情研究会）77 頁以下
[8] クラウド・コンピューティング関連法研究会[2012a]「総論・米国愛国者法」NBL976 号 10 頁
[9] クラウド・コンピューティング関連法研究会[2012b]「個人情報保護法制」NBL977 号 68 頁
[10] 夏井高人[2010]「クラウドコンピューティングサービスと営業秘密の保護」情報ネットワーク・ローレビュー9 巻 1 号 93 頁
[11] 園部逸夫編[2005]『個人情報保護法の解説（改訂版）』（ぎょうせい）
[12] 岡村久道[2009]『個人情報保護法（新訂版）』（商事法務）

[44] Mather ほか[2010]156 頁，石井[2012b]439 頁以下など
[45] ファーストサーバ事件については，北岡[2012]，上山＝小川[2012]，吉井[2012]など参照.

[13] 宇賀克也[2009]『個人情報保護法の逐条解説（第 3 版）』（有斐閣）
[14] 三宅弘＝小町谷育子[2003]『個人情報保護法』（青林書院）
[15] 濱野敏彦[2011]「クラウド・コンピューティングの概念整理」寺本振透編集代表・西村あさひ法律事務所『クラウド時代の法律実務』（商事法務）1 頁
[16] Sanjay Ghemawat et al.[2003], The Google File System, ACM SIGOPS Operating System Review Volume 37, Issue 5, p.29
[17] 山本博資[2004]「秘密分散法とそのバリエーション」数理解析研究所講究録 1361 巻 19 頁
[18] 藤村明子ほか[2005]「電子情報の安全性確保と Forensics の社会的実現に向けた秘密分散技術の考察」情報ネットワーク・ローレビュー4 巻 1 号 30 頁
[19] 加藤英雄[2011]『決定版クラウドコンピューティング―サーバは雲のかなた』（共立出版）
[20] NRI セキュアテクノロジーズ編[2010]『クラウド時代の情報セキュリティ』（日経 BP 社）
[21] 鈴木正朝[2004]『個人情報保護法とコンプライアンス・プログラム』（商事法務）
[22] 情報処理推進機構[2010]「クラウド・コンピューティング社会の基盤に関する研究会報告書」〈http://www.ipa.go.jp/about/research/2009cloud/pdf/100924_cloud.pdf〉
[23] 総務省[2010a]「スマート・クラウド研究会報告書」〈http://www.soumu.go.jp/main_content/000066036.pdf〉
[24] 経済産業省[2009]「個人情報の保護に関する法律についての経済産業分野を対象とするガイドライン（平成 21 年 10 月 9 日厚生労働省・経済産業省告示第 2 号）」〈http://www.meti.go.jp/policy/it_policy/privacy/kaisei-guideline.pdf〉
[25] 日経 BP 社出版局編[2009]『クラウド大全―サービス詳細から基盤技術まで』（日経 BP 社）
[26] 総務省[2010b]「クラウドコンピューティング時代のデータセンター活性化策に関する検討会報告書」〈http://www.soumu.go.jp/main_content/000067988.pdf〉
[27] 新保史生[2012]「諸外国の機関と EU の動向」岡村久道編『クラウドコンピューティングの法律』（民事法研究会）399 頁
[28] 石井夏生利[2012]「EU データ保護規則提案と消費者プライバシー権利章典」Nextcom10 号 30 頁
[29] 新保史生[2000]『プライバシーの権利の生成と展開』（成文堂）
[30] 岡村久道＝新保史生[2002]『電子ネットワークと個人情報保護』（経済産業調査会）
[31] 石井夏生利[2008]『個人情報保護法の理念と現代的課題―プライバシー権の歴史と国際的視点』（勁草書房）
[32] 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 33 巻 53 頁
[33] 堀部政男[2010b]「プライバシー・個人情報保護の国際的整合性」堀部政男編『プライバシー・個人情報保護の新課題』（商事法務）1 頁
[34] 経済産業省[2010]「『クラウドコンピューティングと日本の競争力に関する研究会』報告書」〈http://www.meti.go.jp/press/20100816001/20100816001-3.pdf〉
[35] 北川賢一[2009]「クラウドは幻滅期に入るのか，課題克服に向け業界は努力を」〈http://itpro.nikkeibp.co.jp/article/MAG/20091027/339542/〉
[36] 平野美恵子ほか[2002]「米国愛国者法（反テロ法）（上）」外国の立法 214 号
[37] 河上和雄ほか編[2010]『大コンメンタール刑事訴訟法第 2 巻（第 2 版）』（青林書院）〔渡辺咲子執筆〕386 頁
[38] 田口守一[2009]『刑事訴訟法（第 5 版）』（弘文堂）
[39] 田宮裕[1996]『刑事訴訟法（新版）』（有斐閣）
[40] 石井夏生利[2012]「カナダ法制の動向」岡村久道編『クラウドコンピューティングの法律』（民事法研究会）439 頁
[41] 北岡弘章[2012]「データ消失のリスクを低減する方法」Business Law Journal55 号 32 頁
[42] 上山浩＝小川尚史[2012]「クラウドサービス等のトラブル対応」Business Law Journal55 号 37 頁

[43] 吉井和明[2012]「ホスティング，クラウドにおけるデータ消失に関する法的検討」
〈http://www.slideshare.net/kgoodwell/ss-13718680〉