2011.5.26
サイバー犯罪に関する白浜シンポジウム

クラウドサービスの法的解析

弁護士・国立情報学研究所客員教授
岡村　久道

クラウドコンピューティングと東日本大震災

- 津波で流されたり、浸水等のために使用できなくなった情報システムが少なくない。
- 戸籍が庁舎とともに津波で流されてしまった自治体もあり、完全な再製ができるか、不安視する声。これに対し、住民基本台帳データは住基ネット経由でバックアップされていたので、ほぼ復元ができた。
- これまで、情報セキュリティといえば、我が国では、異様なまでに機密性に重点が置かれていた。しかし、今回の事態によって、今後は可用性を重視する方向へと、パラダイムシフトするのではないか。
- クラウドをうまく使えば、通信回線さえ復旧すれば情報システムを使うことができるし、データの喪失を防ぐことができる可能性。

クラウドコンピューティング（Cloud Computing）とは何か？

- IT戦略本部「i-Japan戦略2015」（2009年7月）の用語解説
  - 「データーサービスやインターネット技術などが、ネットワーク上にあるサーバ群（クラウド（雲））にあり、ユーザーは今までのように自分のコンピュータでデータを加工・保存することなく、『どこからでも、必要な時に、必要な機能だけ』を利用することができる新しいコンピュータネットワークの利用形態」
- いわば、インターネットと、それに接続されているサーバ全体を「雲」（cloud）に例えて、インターネットを介してユーザーのコンピュータで利用しようとするもの。
- 技術的な専門用語ではなく、技術専門家間でも定義は確立せず。

The NIST Definition of Cloud Computing Ver.15

(http://csrc.nist.gov/groups/SNS/cloud-computing/cloud-def-v15.doc)

- **Definition of Cloud Computing:**
  - Cloud computing is a model for enabling convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction. This cloud model promotes availability and is composed of five essential **characteristics,** three **service models**, and four **deployment models**.
- **Essential Characteristics:**
  - *On-demand self-service. Broad network access. Resource pooling. Rapid elasticity. Measured Service.*
- **Service Models:**
  - *Cloud Software as a Service (SaaS). Cloud Platform as a Service (PaaS). Cloud Infrastructure as a Service (IaaS).*
- **Deployment Models:**
  - *Private cloud. Community cloud. Public cloud. Hybrid cloud*.

※ **NIST** National Institute of Standards and Technology （米国国立標準技術研究所）

クラウドの定義が持つ意味

- NIST がいう「3つのサービスモデル」
  - SaaS (Software as a Service)、PaaS (Platform as a Service)、及びIaaS (Infrastructure as a Service)
- 現状では、クラウド・コンピューティングといっても、せいぜいインターネット経由でコンピュータリソースを提供するサービスであるという点で共通しているにとどまる。
- 経済産業省「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（2010年8月）
  - 「『ネットワークを通じて、情報処理サービスを、必要に応じて提供／利用する』形の情報処理の仕組み（アーキテクチャ）」と定義するにとどめている。
- クラウドはバズワードという声も強い。

クラウドに関し法的側面からの検討作業が必要な理由

- 従来の場合
  - 従来におけるデータセンターの利用は、ユーザー企業との専用線接続が一般的。このモデルでは、利用されるべきデータセンターは、通信費用との関係で、必然的に近隣の国内に所在するものとならざるをえなかった。
- データの越境
  - これに対し、クラウドではインターネット回線を用いることが一般的。このため、通信費用を考慮しなくてもよいので、必ずしも国内である必要はない。それゆえ、国外事業者の日本国内市場への参入が容易となるので、国内IT産業の空洞化を危ぶむ声があるとともに、サービスやデータをめぐって国際的な問題が生じる。
- データの所在の不明確性
  - さらに、仮想化技術によって、全世界に広がったインターネット上に、無数のサーバ群が接続されており、どこに所在する、どのようなサーバ群からサービスの提供を受けているのか、ユーザー側が把握困難になっているケースすら存在することが、この問題に拍車。
- ここに、従来におけるコンピュータ資源の利用、そしてデータセンターの利用と比べて、クラウドを、改めて法律的に分析すべき最大の理由がある。
- （以下は拙稿「クラウドコンピューティングと法律」情報通信ジャーナル2009年12月号をベース）

どこの国の裁判所で訴訟が起こせるか？

- 当事者（クラウドベンダ・ユーザ企業）間の場合
  - 契約関係が主たる問題
  - 契約で合意管轄条項があることが一般的
  - 一般には約款でクラウドベンダの本国（本店所在地）の裁判所が指定されている
- 公法関係と、強制捜査など法令の執行
  - 問題にもよるが、捜索・差押え等はデータセンター所在地国の裁判所による
  - 強制捜査のような場合、執行地の裁判所が令状を発布し、他国の裁判所は原則無関係
  - よって、契約ではコントロールできない

どこの国の法令がクラウドに適用されるか？

- クラウドベンダ・ユーザ企業間の権利義務
  - 契約関係が主たる問題
  - 当事者の合意（準拠法の指定）によって決められる
  - 当事者間における力関係の問題だが、一般には約款でクラウドベンダの本国法（本店所在地法）が指定されている
- 公法関係と、強制捜査など法令の執行
  - 問題にもよるが、捜索・差押え等は、データセンター所在地国の法律による
  - 捜査機関等の官憲によるトラヒックの傍受は、サーバや回線が存在する国の法律による
  - 強制捜査のような法令の執行は、執行地の国家機関による
  - 他国の国家機関は原則執行できない
  - よって、契約ではコントロールできない
  - データセンター所在地国等が変更されるたびに、どこの国の公法がクラウドに適用されるかについても変化

クラウドベンダ・ユーザ企業間の契約

- 契約の重要性
  - 個々のクラウド・サービスの内容は多様であるが、各提供契約によって決まっている。よってクラウドベンダとユーザー企業との関係では、サービス提供契約の内容こそが最も重要。
- SLA（Service Level Agreement）
  - 契約内容については、提供するサービスの水準を示したSLAと呼ばれる契約で、サービス内容の詳細が定められることが一般的。
- 附合契約が一般的
  - 契約の大量処理の要請から、ベンダ側が一方的に契約の約款内容（オプションサービスを含む）を決めておくという傾向。
  - ユーザー企業からすると、条項に関する契約交渉の余地が少なく、その採否しか決定できない場合が多い。
- ユーザー企業の観点から
  - 導入決定に先立ち、契約内容を詳しく吟味しておき、採否・利用範囲を決定することが重要。

契約内容とカスタマイズ

- 業務内容との合致
  - 提供されるサービス内容が、それによって運用しようとするユーザーの業務内容と合致するものであることを、確認しておかなければならない。
  - 自前のシステムを構築する場合と比べて、どうしてもカスタマイズの自由度は低くなってしまうので、事前に詳細な検討を要する。
- カスタマイズの可否
  - 多くのカスタマイズを要する場合には、クラウドの恩恵を十分に享受することができない（トレードオフの関係）。
  - 特別な保守費用やメンテナンス費用を支払わなければならない場合もある。どのような規定になっているか、確認を要する。
  - 他のクラウドベンダへと移行しようとする場合には、すでにカスタマイズのために掛けた費用が、水泡に帰す場合もある。

外字対応の問題

- 我が国では、特に氏名等について外字の使用が避けられない。
- Shift-JISと比べてUnicodeを使っていれば必要な外字の数は減るが、Unicodeでもすべての戸籍文字はフォローできていない。
  - 同定済みでも未コード化の戸籍文字が3万字以上（総務省）。
  - 外字の使用を要する場合、移行予定先のクラウドが、外字に対応しているか、対応方法の内容を含めて確認作業が必要。
  - 経済産業省で文字コード化を検討中。
- クラウドに移行する際、元のレガシーシステムで用いられてきた外字が、各ベンダの独自仕様、そして各使用組織の独自定義となっているケースが一般的。
  - 未コード化の外字について、クラウドへの移行に先行して同定作業が必要。
  - 構築・運用中の組織的な外字管理が必要。
  - 総務省・自治体クラウド推進本部有識者懇談会でも対応方法を検討中。
- 対応を怠るとシステムやデータの可用性・完全性を害するおそれ。

契約の終了ーポータビリティ等に関する課題

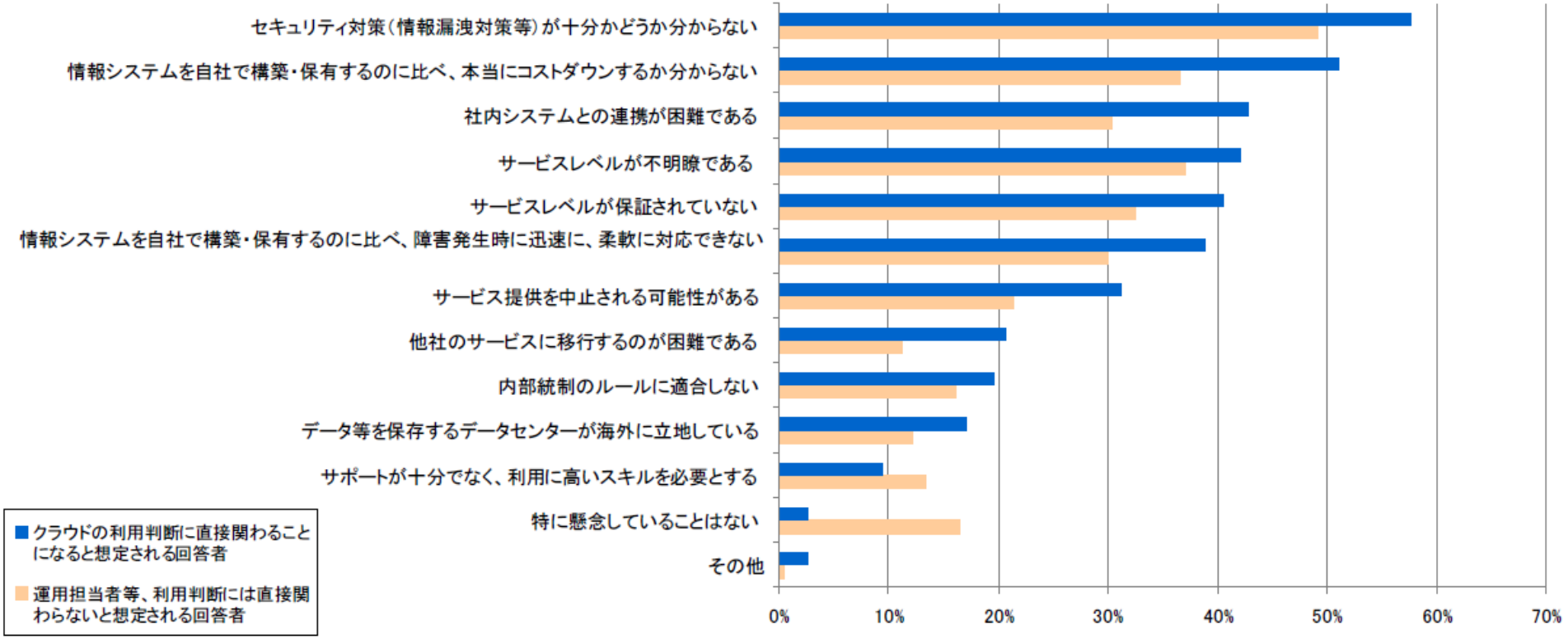
- ユーザーが、すでに契約しているサービスから、別のクラウドベンダが提供する新サービスへと乗り換えようとする場合、旧サービス提供契約を解約して、データを新サービスに移行する必要。
- ところが、旧サービスのデータ形式が独自、もしくはデータの書き出しが困難な場合には、事実上、新サービスに移行できない（ベンダロックインーベンダによる顧客の囲い込み）。
- サービス提供事業者の倒産時にも、同様の問題が発生。
- ユーザーがデータのポータビリティを保つためには、契約期間中に入力、集計、加工したデータをユーザーが契約終了時に出力して受領する権利の有無と条件、どのようなデータ形式での出力の可否、その容易性はどうか等の点が、どのように定められているかについて、契約締結時に検討しておく必要。
- 併せて、漏えい防止のため、提供事業者側に契約終了時のデータ消去義務が定められているか等についてもチェックが必要。
- 相互運用性も重要な場合あり。

情報セキュリティ上の留意点

- クラウドでセキュリティが特に問題となる理由
  - クラウドコンピューティングの構造上、漏えいをはじめ、預けているデータ、サーバのハード・ソフト等の安全性は、主としてサービス提供事業者側のセキュリティレベルに依存せざるを得ない点に特徴。
  - ところが、データセンターがどこの国に置かれているのかも不明な場合がある。
  - しかもオープンなインターネット回線を利用するときは、それによるリスクもある。
- 経済産業省「SaaS向けSLAガイドライン」（2008年1月）
  - データの格納形態（分散化、暗号化有無など）の確認、障害時の復旧範囲（復旧できるデータとできないデータの種類）、復旧に要する時間、自社のデータにアクセス可能な提供者スタッフ数の最小化、アクセスできるデータの範囲などに関してSaaS 提供者と取り決めを事前に締結しておくことが大切である。」等とする。
  - 他にも多くの点に触れている。
- SLA等の関連契約条項で、どのように定められているか、導入決定前に検討が必要。

クラウド・コンピューティングを利用する際の懸念

（経済産業省「情報システム・ソフトウェアの信頼性及びセキュリティの取組強化に向けて－中間報告書－」（「高度情報化社会における情報システム・ソフトウェアの信頼性及びセキュリティに関する研究会」平成21年5月）



「クラウド・コンピューティングを利用する際の懸念として「セキュリティ対策が十分かどうかわからない」、「サービスレベルが不明瞭である」などの回答が多く挙げられており、クラウド・コンピューティング利用において信頼性・セキュリティへの不安が大きな課題となっていることが伺える」（上記報告書）

契約違反と救済の問題

- サービス提供事業者側に責任減免条項が定められているケースが多い。
- 現実に障害が発生した場合に、ユーザー側で原因を特定することが困難となるおそれ。
  - クラウドは、ブラックボックス化、多層化された「雲」であるため、責任の切り分けが困難。
  - サーバ所在国すら不明な場合がある。
  - いきおいサービス提供事業者側が示した説明を鵜呑みにするほかない状況へ追いやられ、SLA上の責任追及が困難になるおそれ。
- 履行補助者
  - 原因が特定された場合には、クラウド側で発生したインシデントは、たとえ提供事業者が当該サービスの運用の一部を委託しているサードパーティに起因するものであっても、当該サードパーティは提供事業者の履行補助者として、提供事業者の責任となる。
- しかし、提供事業者が海外事業者の場合、合意裁判管轄条項、準拠法の指定のため訴訟提起が困難になるおそれはないか？

契約によるコントロールの限界

- サーバ所在地国に関するリスクはないのか？
  - サーバ所在地国のカントリーリスクが生じる場合があるだけでなく、その国の法令によって、当該国の政府に対して通信のデータ内容等の開示義務が課されているような場合には、データの機密性は保たれない。
  - 海外のクラウドベンダの中には、サーバ所在地を明らかにしていないケースもあり、そうなれば、どのような国の法令に服するのかを含め、カントリーリスクについてリサーチすらできない。
  - サーバ所在地国を明らかにしているケースであっても、サーバ所在地の移転が自由に認められていれば、契約時に想定していなかった国のカントリーリスクに、新たに服することになるリスクがある。
- データ通過地国に関する同様のリスクの有無は？

USA Patriot Act（愛国者法）

- テロ対策等の目的で、捜査機関に広く通信傍受等の権限を付与した法律
- 2009年4月、FBが、米国のデータセンターを捜索してサーバ等のT設備を押収。そのため、同一データセンタを利用していた約50社がメールやデータへのアクセスが不能になった。
- 他国の法律でも通信傍受を広く認めるものがある。

コンプライアンス等への適合性

- 法令でデータの取扱いに関する責任を定めているケース（例：個人情報保護法制）があり、特定のクラウドを利用した場合に、それらの法令に適合しているといえるか、確認が必要。
- 個人データの越境流通として、EU個人データ保護指令への適合性を要するケースも想定される。
- システム監査との関係も不明。

外国為替及び外国貿易法

- 特定の技術を特定の外国において提供する際や特定の外国人・外国企業に提供する際には、経済産業大臣の許可が必要。
- 25条3項
  - 特定国において受信されることを目的として行う電気通信による特定技術を内容とする情報の送信」も許可の対象。
- したがって、日本国内から海外の外部サーバに情報を送信する際や、当初から外国の利用者に情報を提供することを目的に自社の海外サーバに情報を送信する際、国内サーバのリソースを演算処理等のために提供してその結果を送信する際等も、許可の対象となる場合がある。この特定技術とは、核兵器等の大量破壊兵器や通常兵器に関連した技術を指しており、例えばこの技術の中には暗号技術などの汎用的な技術も多く含まれるため、これらの情報を取り扱う際には留意が必要（経済産業省「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（2010年8月））。

個人情報保護法とクラウドベンダ

- クラウド事業者は個人情報取扱事業者に該当するか？
  - 取り扱う個人データが過去6ヵ月で一度でも5000人分を超えれば個人情報取扱事業者に該当。
  - これはクラウドベンダが事業全体で取り扱う個人データの頭数によって決せられる。
  - クラウドベンダのサーバ内にユーザー企業が保有する個人データは、クラウドベンダにとって「取り扱う」ものとはならず、5000人分の算入対象外となるのではないか？
  - 仮に算入対象外となるとしても、他の事業で取り扱う個人データの頭数が5000人分を超えれば、クラウドベンダは個人情報取扱事業者に該当する。
- クラウド事業者が個人情報取扱事業者に該当する場合
  - クラウドベンダのサーバ内にユーザー企業が保有する個人データが、クラウドベンダにとって「取り扱う」ものとならないのであれば、当該クラウドベンダは当該個人データについて、個人情報保護法上の義務を負わない可能性がある。しかし、この点の解釈は未確立。
  - クラウドベンダが、自らの事業のために、預かっている個人データを独自に利用すれば、保護法上の義務が課せられる。

個人情報保護法とユーザー企業

- ユーザー企業が個人情報取扱事業者に該当する場合を前提に個人情報保護法との関係を検討
- ユーザー企業がクラウド上に個人データを置く行為
  - は第三者提供（23条）に該当する可能性があるが、少なくとも「委託」に該当するので、本人の事前同意は不要。
  - その代わりとして、ユーザー企業はクラウドベンダに対する監督義務を負う（22条）。
  - クラウドについて、監督義務を果たすものと認められることができるか？
  - 以上の点は、SaaS (Software as a Service)、PaaS (Platform as a Service)、及びIaaS (Infrastructure as a Service)で異なるか？

EU95年データ保護指令25条との関係

- EU95年データ保護指令25条に基づき、EU域内諸国はデータ保護の十分性がない国へのデータ域外移転に関する制限を法整備。
- 現時点で我が国は「十分性」を認められていない。
- そのため、EU域内の現地法人が、クラウドによってEU域外に個人情報を域外移転することになるケースでは、当該個人情報保護に関する法律によって、域外移転のための手続が求められることになる。

カナダ・ブリティッシュコロンビア州 個人情報保護法

- Freedom of Information and Protection of Privacy Act [RSBC 1996 Chapter 165] (B.C. FIPPA)）30.1条
- **Storage and access must be in Canada**
- **30.1 A public body must ensure that personal information in its custody or under its control is stored only in Canada and accessed only in Canada, unless one of the following applies:**
- **(a) if the individual the information is about has identified the information and has consented, in the prescribed manner, to it being stored in or accessed from, as applicable, another jurisdiction;**
- **(b) if it is stored in or accessed from another jurisdiction for the purpose of disclosure allowed under this Act;**
- **(c) if it was disclosed under section 33.1 (1) (i.1).**

- 公的機関等は、自己の保持・管理に係る個人情報については、個人の同意等の要件に該当する場合を除き、カナダだけで保管、アクセスされるようにする義務を負う。

個人情報保護に関するその他

- 総務省「ASP・SaaS 事業者が医療情報を取り扱う際の安全管理に関するガイドライン」（平成21年７月）
  - 「所管官庁に対して法令に基づく資料を円滑に提出できるよう、ASP・SaaS サービスの提供に用いるアプリケーション、プラットフォーム、サーバ・ストレージ等は国内法の適用が及ぶ場所に設置すること。」

データ流出とプライバシー侵害の例

- ヤフーBB事件
  - 総合電気通信サービスを運営する会社からの漏えい事件。
  - 社外からのメンテナンス作業のためにリモートメンテナンスサーバを設置。同サーバの中にヤフーから預かった顧客データベースとして原告らの氏名・住所等の個人情報を保有管理。
  - 業務委託先から派遣されていた甲に、同サーバを含むサーバ管理業務を行わせ、共有アカウントを与えていた。
  - ところが、甲の退職後も同アカウント等の変更を行わなかったため、甲と第三者乙が共同もしくは単独で同アカウントを用いて不正アクセスして顧客データベースのデータを不正取得し、もって外部流出。
- 大阪地裁平成18年5月19日判決
  - ユーザー名・パスワードの管理が極めて不十分であったことなど、外部からの不正アクセスを防止するための相当な措置を講ずべき注意義務を怠った過失により原告らのプライバシーの権利が侵害されたとして、不法行為責任を認めた。
- これを控訴審判決も支持

著作権侵害とストレージ事業者の責任

- 事案
  - ユーザーが、自己の所有するCDの楽曲をパソコンで圧縮ファイル化してネット上のサーバにアップロードしておき、自己の携帯電話にダウンロードして再生するためのストレージサービス事業に関するもの。
- 東京地裁平成19年5月25日判決
  - アップロードによる複製、ダウンロードによる通信の行為主体が、ユーザーではなくサービス提供事業者であって、「ユーザーは複製のための操作の端緒となる関与」をしたにとどまると判示。
  - 本件サービスでは「本件サーバへの複製行為が不可避的」で、こうした「中心的役割を果たす本件サーバ」は、サービスを提供する事業者が「所有し、その支配下に設置して管理」し、サービスの仕様等も事業者側のシステム設計で決定されていることなどを、主たる理由とする。
- 問題点
  - 当該電気通信事業者のサーバがサービス提供のための中心的役割を果たしている。その他の点を含め、この判決が示した前記理由は、こうした情報通信サービス全般に当てはまる特徴を、単に網羅しただけのものにすぎない。
  - この理屈によると、多くのクラウドサービスで、クラウドベンダは著作権侵害の主体となりかねない。

サービス提供事業者と利用範囲に関する選定作業の重要性

- 自社の事業に適合しているものを選択する必要
- 何らかの原因でサービスが利用できなくなれば、それを利用していたユーザー側の業務も停止。
  - 提供事業者の倒産や、戦争・クーデター等による通信途絶をはじめサーバ所在国のカントリーリスク等を想定することが必要。
- それゆえユーザー側としてはクラウドベンダの選定と利用範囲の選定が重要。
- クラウド・アセスメントとでも呼ぶべきもの。

その他の問題

- 不正競争防止法の営業秘密保護との関係
- 情報セキュリティ規格との関係
- その他