Cloud Computingと情報セキュリティ ー法令・契約の観点から

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（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。
  - 主として後述のSaaS、PaaSを中心としており、IaaSまでをも含めて使われることもあり（米NISTにおけるクラウドの分類）。
- 主としてインターネット経由の情報処理サービス提供という点で共通。
- そのためサーバ所在地も国内である必要性がなく、国外事業者の日本国内市場への参入が容易。

2

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）

3

検討作業の必要性等

- 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いることから、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きていることが特徴。
- 普及を支える要因（自前システムの構築と比較した利点）
  - ブロードバンドや携帯電話による情報通信の接続環境が整備されて低価格化していること
  - 企業におけるコストダウンの要請
  - 企業活動の迅速化の要請等
- すでに公的部門でも一部でサービスの利用が開始。
- 以上の点等を考慮すると、今後、さらに普及するものと推測されるので、情報セキュリティ上の課題の有無と内容に関する検討が必要であるが、サービス提供契約、及び、関連法令等との関係でも検討作業を要する。

4

SaaS（Software as a Service）

- サービス提供事業者側が運用するサーバ上でソフトウェアを稼働させ、インターネットを経由で、ユーザーにブラウザ等で利用させるという形態のサービス。いわば仮想アプリケーションサービス。
- 一般的にはASPの同義語として使われるが、より柔軟なカスタマイズ等を可能にする点でASPの発展形であるといわれることもある。
- 代表的なサービスとして、Googleが提供するGoogle Apps、salesforce.comが提供するSalesforce CRM等。

5

SaaSの利点と課題

- 利点
  - 自前のシステムと比べて、導入、運用等の手間と時間を省くことができる。なお、ハウジングは設置場所のみ。それに加えてホスティングはハードウエア。さらに、それに加えてSaaS はソフトウエアも、提供事業者側が用意。
  - コスト面における利点。実際に使用した限度で利用料を支払えば足り、初期投資が不要である等。
  - 急なユーザー数の増減等にも柔軟な動的対応が可能。
- 課題
  - ユーザー側がブロードバンド環境でなければ、十分な利用ができないものもある。
  - ユーザー側もしくは事業者側の接続障害や、サーバの稼働に障害が発生した場合も同様。
  - インターネットを経由するため、情報セキュリティの点でも不安。
  - オーダーメイドでないため、個々のユーザーの要望に即した弾力的な仕様等の変更も困難になりがち。

6

PaaS（Platform as a Service）

- インターネット経由で提供されるサービスであるという点ではSaaSと類似。
- SaaSが既存のソフトウェアを、限られた範囲でカスタマイズできるだけであるという限界があったのに対し、PaaSはサービス提供事業者側のサーバ上でユーザーのシステムを稼働させられる点で、SaaSの発展形といわれている。それを可能にするために、サービス提供事業者側が事前に開発環境等を提供しておき、これをユーザー側が利用することができる。したがって、カスタマイズの自由度が比較的高い点を除けば、基本的にはSaaSと利点・課題も同様。

7

IaaS（Infrastructure as a Service）

- これもインターネット経由のサービス。
- 仮想化技術を用いてシステムのインフラをネット経由で提供するという点でSaaSやPaaSと異なる。それらと比べてユーザーの自由度が高い。
- サーバ仮想化によるコストダウン進む。
- HaaS（Hardware as a Service）と呼ばれていたサービス形態（単なるハードウェアリソースのインターネット経由の提供サービス）の発展形であるといわれている。このような自由度と導入、運用等の手間と時間の省略とは、トレードオフになりがち。

8

クラウドコンピューティングと法令に関するフレームワーク

- 契約内容に関する法的課題
  - いずれの形態に属するものであっても、サービス提供契約である点で共通しており、しかも形態は多様なので、契約内容によって決定される部分がほとんど。
  - 各サービスごとに、付合契約型のもの（オプションサービスを含む）が多く、条項の自由度が低いという傾向。
  - 契約内容についての検討事項は何か？
- 契約内容以外の法的課題
  - インシデント発生時に、契約に基づく救済が実際に受けられるか？
  - サービス提供事業者の倒産等によるサービス提供停止への対応は？
  - 情報セキュリティ関連の法令、規格、監査上の要求事項と合致するのか？
  - 所在地国の法令による機密性侵害のおそれはないのか？
  - その他の問題

9

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

- 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。
  - ユーザーの業務に使用する場合、システムを稼働させるプログラムだけでなく、当該業務に関するすべてのデータも、ユーザー内ではなく、サービス提供事業者側のシステム内に収容されてしまうという点に共通性。
  - データセンターと専用回線でつなぐ場合には、通信料金との関係で距離が近い国内であることを要するが、インターネットを経由するクラウドの場合には国外でも変わりがない。そのため、国外事業者の参入が容易であり、サーバ設置場所は国外であることが多い。
  - したがって、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サービス提供事業者の選定と利用範囲の選定が重要。

10

省庁公表のクラウド関連ガイドライン

- 提供するサービスの水準を示したService Level Agreement（SLA）に関係して、省庁が関連ガイドラインを公表。
- 経済産業省「SaaS向けSLAガイドライン」（2008年1月）
  - SLAに関し、望ましいサービス内容とその具体的設定例について検討。
- 総務省「ASP・SaaS における情報セキュリティ対策ガイドライン」（同月）
  - ASP・SaaS 事業者がASP・SaaS サービスを提供する際に実施すべき情報セキュリティ対策を対象とするもの。

11

参考－標準化団体等の動向

- 米国
  - Open Cloud Manifesto
    - http://www.opencloudmanifesto.org/
    - IBM、Sun等
  - Cloud Security Alliance（CSA)
    - http://www.cloudsecurityalliance.org/
    - eBay等
  - Open Cloud Consortium(OCC)
    - http://opencloudconsortium.org/
    - Cisico、Yahoo等
- 日本
  - 日本OSS推進フォーラム
    - http://www.ipa.go.jp/software/open/forum/index.html
    - OSS 系。IPAが事務局。
  - ASP･SaaSインダストリ･コンソーシアム（ASPIC）
    - http://www.aspicjapan.org/index.html

12

情報セキュリティ上の留意点

- 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。
- 前掲経済産業省ガイドライン
  - 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。

13

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。

14

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、別の事業者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。

15

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？

16

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。
  - 海外の提供事業者の中には、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？

17

法令の執行との関係等

- サーバ所在地国の法執行機関によって、日本の政府や地方公共団体が有するデータが捜索・差押の対象とされてしまうリスクはないのか？
- サーバ所在地国でインシデントが発生した場合に、日本の法執行機関の権限が及ばないことを、どのように考えるべきか？
- 準拠法の指定次第では、外国法に服することにならないか（実際に米国法を準拠法として指定しているケースあり）？
- 裁判管轄の指定次第では、国外の裁判管轄に服することにならないか（実際に米国を裁判管轄としているケースあり）？
- サーバ所在地国や通過地国の法令について、結果として、日本の政府や地方公共団体が違反していたという事態は生じないか？

18

その他の問題

- 国外のクラウドに依存している場合、通信途絶等によって政府・公共団体の機能等が麻痺してしまうおそれはないか？
- クラウドの普及は国内情報処理産業の空洞化を招かないか？
- 国内情報処理産業の国際競争力強化のための課題は何か？
- クラウドの普及によって国外への依存度が高まることによって、他にもリスクが生じないか？
- むしろ、国外事業者を含めて、ブロードバンド網が整備された国内へと誘致する仕組みが構築できないか、そこに電子自治体機能を担わせることができないか？

19