サイバースペース 法律相談所 第66回

クラウドコンピューティングと契約

[今月の回答者]
岡村久道 弁護士

Q **当社は従来から自前の情報システムを構築・運用して業務を行ってきましたが、最近、クラウドコンピューティング・サービスに乗り換えるよう勧誘を受けました。どのような意味の言葉なのでしょうか。導入を検討する際に注意すべき点は何でしょうか。**

A 「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」です。しかし、サービスごとに内容は一致しておらず、サービス提供契約によって決まりますので、導入の際には、利点と欠点とを吟味して、導入する業務の対象を合理的に絞り込んだ上、しっかりした提供事業者の選定と、契約条項の十分な確認が必要となります。

解説

●クラウドコンピューティングとは何か

最近では「クラウドコンピューティング」（Cloud Computing）という言葉を耳にする機会が増えてきました。政府のIT戦略本部が2009年7月6日に公表した「i-Japan戦略2015」にも、「電子政府・電子自治体クラウド」等の記載が見られます。冒頭の「A」で述べた定義も、この戦略に添付された用語解説に基づいています。

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）に見立てた上、この「雲」を、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です。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、ユーザー側が把握できなくなってきていることを背景としています。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、企業における経費削減の動向等も、クラウドの普及を支える要因です。

この言葉はGoogleのエリック・シュミットCEOによって2006年に提唱され、現在では同社や、salesforce.comのような新興企業だけでなく、Amazon、IBM、Microsoft等の米大手ICT企業も、軒並みサービスに参入しています。わが国の郵便局株式会社も、すでに米国系のクラウド事業者が提供するサービスを利用しています。

しかし、この言葉は技術的な専門用語ではありません。技術専門家の間でも定義はバラバラです。後述のSaaS、PaaS、そしてIaaSまでをも含めて使われることもあり、せいぜいインターネット経由のサービス提供という点で共通しているだけです。そのため、クラウドという言葉は人々を混乱させるだけだという声もあります。まさに「雲を掴むような話」です。それは主として営業的な観点から提唱されている言葉という側面があるからです。そのため、すでに死語に近づいた流行語「Web 2.0」の二の舞となる可能性もあります。

出典：『情報通信ジャーナル』 2009年12月号
財団法人電気通信振興会の許可を得て複製

少し前置きが長くなりますが、以下では先にSaaS等について説明した後、契約等の注意点を解説します。

SaaS (Software as a Service)

SaaSとは、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ておき、インターネットを経由して、それを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です。無料のものもありますが、企業向けサービスの大半は有料です。一般的にはASP (Application Service Provider) の同義語として使われていますが、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ります。代表的なSaaSのサービスとして、Googleが提供するGoogle Apps、salesforce.comが提供するSalesforce CRM等があります。

ユーザーが優れたSaaSサービスを選んで上手に利用すれば、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ます。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の点で、コスト面における利点もあります。急なユーザー数の増減等にも柔軟な動的対応が可能です。これによるICTの「所有」から「利用」へという流れも指摘されています。

しかし、これらの利点の半面として、幾多の欠点もあります。例えば、ユーザー側にインターネット接続がなければ利用できず、ブロードバンド接続環境でなければ十分な利用ができないものもあります。

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です。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が残ります。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です。これらの点については、改めて後述します。

PaaS (Platform as a Service)

次に、PaaSは、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と類似しています。やはり無料のものもありますが、通常は対価としてユーザーが利用料を支払う形態です。

SaaSが既存のソフトウェアを、せいぜい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て、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ることもできる点で、SaaSの発展形であるといわれています。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ます。したがって、カスタマイズの自由度が比較的高いという特色があります。しかし、その点を除けば、基本的にはSaaSと利点・欠点も同様です。

代表的なサービスは、salesforce.comが提供するForce.comプラットフォーム、Googleが提供するGoogle App Engine等です。

IaaS (Infrastructure as a Service)

これもインターネット経由のサービスです。やはりSaaSについて述べた利点・欠点が、IaaSにも基本的にあてはまります。

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と異なっています。それらと比べてユーザーの自由度が高い点が売り物です。かつて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ます。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、得てしてトレードオフの関係になりがちです。

Amazon.comが提供するAmazon EC2 (Elastic Compute Cloud)、S3 (Simple Storage Service) 等が、現時点におけるIaaSの代表的なサービスです。

サービス提供事業者と利用範囲の選定

以上のSaaS型、PaaS型、IaaS型の別を問わず、クラウドコンピューティングは、サービス提供事業者側のサーバ上で稼働するサービスを、ユーザーがインターネット経由で利用するという点で共通しています。したがって、これを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、自社内ではなく、「雲の中」(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でも共通しています。そのため、基幹業務に使用する場合には、通信障害や提供事業者のシステム障害が起これば、ユーザーの基幹業務も停止して、ユーザーの

経営が立ち行かなくなるおそれも発生します。サービス提供事業者が自社の競争会社に企業買収されるケースも想定されます。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についても、後述の契約条項の整備だけではまかないきれません。万一の際に、うまくデータを救出できても、他の提供事業者への乗り換えが完了できるまでの間は、当該業務が停止してしまい、莫大な損失が発生するおそれがあります。

そのため、ユーザー側の事業継続性計画という観点から、提供事業者の選定が重要になります。ユーザー側としては、事前に提供事業者に関する選定基準を用意しておき、それを提供事業者の概要や契約内容と対比して選定することが重要です。

同様の観点から、どのような業務にクラウドを利用するか、利用範囲の選択についても吟味することが必要です。扱うデータの重要性等に応じて選択すべきことになります。パブリッククラウドとプライベートクラウドを使い分けるという視点も提唱されています（総務省「スマートクラウド研究会（第1回）」におけるNTTデータ作成の一般公開配布資料参照）。

●クラウドコンピューティングと契約

クラウドコンピューティングについては、国内外で標準化に向けた動向が生じていますが、現時点では標準化に至っていません。このような背景で、前述のような共通点があるといっても、具体的な内容――SaaS、PaaS、IaaS等の形態の別と諸条件――は、個々のサービス提供契約の内容によって決まっており、しかも、その内容はバラバラであるのが現状です。対価の基準についても同様です。これらの点でもサービス提供事業者の選定が大きな意味を持つほか、契約内容こそが最も重要となります。

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（Service Level Agreement）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です。

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、経済産業省から「SaaS向けSLAガイドライン」（2008年1月）が公表されています。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として、総務省から「ASP・SaaSにおける情報セキュリティ対策ガイドライン」（同月）も公表されています。

これらのガイドラインに示された考え方の多くは、SaaS型だけでなく、PaaS型や、IaaS型のクラウドにも該当します。以下では、これらのガイドラインを参考にしつつ、筆者独自の観点から、クラウドコンピューティングに関する契約上の課題について解説します。

●カスタマイズの可否等

まず、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りません。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いますので、事前に詳細な検討を要します。

一般的には、SaaS型よりもPaaS型の方がカスタマイズの自由度が高いといっても、個々のサービスによってまちまちであることも事実です。大幅なカスタマイズでも要求を満たせないときは、IaaS型クラウドを選択せざるを得ません。

導入、運用等の手間と時間を省くことができ、初期投資が不要であるというSaaS型やPaaS型の利点は、多くのカスタマイズを要する場合には、その恩恵を十分に享受することができません。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りますので、どのような規定になっているか、確認を要します。しかも他のサービス提供事業者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ります。

いずれにしても、カスタマイズの自由度と条件を、事前に確認しておく必要があるはずです。

●情報セキュリティ上の注意点

SaaS型をはじめ、クラウドコンピューティング・サービスの提供を受けるということは、自社データを外部に預けるという意味になりますので、情報セキュリティの確保が重要になります。

もちろん自社でデータを保管する場合でも、情報セキュリティを維持しなければならない点では変わりが

ありません。しかし、クラウドコンピューティングの構造上、漏えいをはじめ、預けているデータの安全性は、主として提供事業者側のセキュリティレベルに依存せざるを得ません。このような見地から、前記経済産業省ガイドラインは、「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。」としています。

他にも、データ等のバックアップ体制は重要です。クラウドコンピューティングの性格上、オープンネットワークであるインターネット上において、サービス提供事業者側のサーバとユーザーとの間で頻繁にデータが送受信されるので、送受信時における暗号化の可否とレベル、VPN、NGN等の利用の可否と条件も重要となります。

提供事業者側でプログラムを自動的にバージョンアップしてくれることは、ユーザーにとって負担が減るので便利なように見えますが、そのために互換性に支障が生じ、システム障害が発生するおそれもあります。

●コンプライアンス等への適合性

最近では法令でデータの取扱いを定めているケースがあり、特定のクラウドを利用した場合に、それらの法令を遵守したといえるか、確認が必要になります。

わが国の個人情報保護法は、個人情報の取扱いについて厳格なルールを定めています。特に個人データの取扱いを委託する際には、委託元の委託先に対する安全管理措置に関する監督義務を明定しています（同法22条）。クラウドでの個人データの管理が委託に該当するかどうかについては見解が一致していませんが、少なくともユーザーである企業そのものが個人データの安全管理措置義務を負うことには変わりがなく、監督官庁のガイドラインが具体的に講じるべき管理策を明らかにしています。したがって、クラウドで個人データを扱う場合、ユーザーである企業としては、この義務を遵守できているか、SLAに即して事前に確認しておかなければなりません。漏えい等の発生時に主務官庁による報告徴収に応じられるよう、ログの取得・保存等についても併せて確認します。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ます。

自社の技術ノウハウ等は不正競争防止法の営業秘密として保護されます。しかし、保護してもらうためには、同法にいう「秘密として管理していること」という要件を満たす必要があります。したがって、自社の営業秘密をクラウドで扱う場合には、この要件を満たしているといえるか、やはりSLAに即して事前に確認を要します。

会社法と金融商品取引法は、それぞれ内部統制について規定を置いています。自社の重要情報をクラウドで扱うことが、これらをクリアできているのかについても、やはり確認が必要です。

法令だけでなく、自社が認証を取得し、もしくは取得を予定しているISO/IEC 27001（ISMS）やJIS Q 15001（プライバシーマーク）の要求事項を満たしているかについても確認を要します。満たしていなければ、当該認証の新規取得や更新が不可能になります。

●ポータビリティと相互運用性に関する注意点

より良い条件の新サービスが出現したために、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ケースは少なくありません。その場合には、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があります。

ところが、旧サービスのデータ形式が独自のものであり、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ません。これは「ベンダロックイン」（ベンダによる顧客の囲い込み）と呼ばれる問題です。サービス提供事業者の倒産時にも、同様の問題が発生します。

このようなベンダロックインの罠に陥ることなく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があります。併せて、漏えい防止のため、提供事業者側に対し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を要します。

また、自社で同時に利用する予定の複数のクラウド間や自社システムとの間で相互運用性が保てるかどうかについても、重要なポイントとなります。したがって、使用可能な入出力フォーマット等についても、確認しておきたいところです。

●契約違反と救済の問題

事業者側が契約違反をした場合に、厳格な責任減免条項が定められているケースは論外ですが、そうでなくても、契約違反の場合に、実際に責任を追及して救済を受けることが可能なのか、という問題もあります。

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、契約条項が適正に遵守されているか、検証することは日常的にも困難です。まして、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できず、責任の切り分けが困難となるおそれがあります。「サーバ所在地国の通信途絶が原因である」など、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、これではSLA上に定められた約束事項も、「画に描いた餅」になりかねない可能性もあります。

次に、幸運にして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なりますので、提供事業者の責任となりそうです。

しかし、これは日本法が適用された場合に通用する話にすぎません。準拠法の指定（どこの国の法令が適用されるのかという問題）に関する規定が置かれており、それによって他の特定の国の法令が適用されると定められている場合には、その国の法令次第となります。サービス提供事業者は海外事業者が多く、その本国の法令が準拠法として指定されていることが少なくありません。

裁判管轄に関する規定も重要です。損害額が高額とはいえないようなときは、わざわざユーザーが、米国の弁護士を立てて米国の裁判所に出訴しようとすると、裁判が費用倒れとなるおそれがあることに、注意しなければならないでしょう。このように、契約に規定されているということと、それを実際に執行できるのかということとは、別の問題であると考えるべきです。

●その他の条項

外国企業が提供するものである場合には、サポート時間についてユーザーの業務時間と合致していることも重要です。

●契約によるコントロールの限界

以上のような契約によるコントロールには限界があります。例えば、サーバ所在地国の法令によって、当該国の政府に対して通信のデータ内容を開示しなければならない義務が課されている場合には、データの機密性は保たれません。事業者によっては、サーバ所在地国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、リサーチすらできません。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法令に、新たに服することになるリスクがあります。以上のようなサーバ所在地国の問題は、その国の法令だけにとどまりません。戦争・クーデター等による通信途絶のようなカントリーリスクも存在していることは、すでに説明したとおりです。

●おわりに

以上のとおり、クラウドの導入に際しては、利点と欠点とを吟味して、導入する業務の対象を合理的に絞り込んだ上、しっかりした提供事業者の選定と、契約条項の十分な確認が必要となります。

Profile

〈おかむら・ひさみち〉京都大学法学部卒業。弁護士（英知法律事務所代表）。国立情報学研究所客員教授。神戸大学法科大学院でも知的財産権法の講座を担当。博士（情報学）。専門は情報法、知的財産法。総務省「情報通信行政・郵政行政審議会」委員。内閣官房IT戦略本部「IT戦略の今後の在り方に関する専門調査会」委員。他にも内閣官房情報セキュリティセンター、内閣府、経済産業省などの委員を歴任。ベストセラーとなった『これだけは知っておきたい！個人情報保護』（日本経済新聞社）ほか、著書多数。