# クラウドにおけるセキュリティーと制度上の課題

二木 真明　住商情報システム株式会社 新規事業開発室 テクニカルアドバイザー

## 契約や法制度上の問題に対するガイドライン作成が急務
## 「データが国境を越える」クラウドでは国際間の合意形成は必須

クラウドコンピューティングの定義についての議論は一段落しつつあるが、定義がはっきりするにつれて、鮮明になってきた課題もある。まず「クラウド」という言葉で、一般の利用者がもっとも不安に感じるのが、「セキュリティー」の問題だ。クラウドの基盤となっている技術は、仮想化、大規模分散処理などだが、これらの技術的な問題点はほぼ既出だ。さらにアプリケーションのレイヤーでも、ウェブアプリケーションの脆弱性問題に見られるように、すでに多くの問題が明らかにされている。クラウドにおけるセキュリティー問題は、ファシリティーの物理的なセキュリティーや、マネジメントサイクルの確立も含めて、既出の問題の延長上にあるのだと思う。ただ、その形態に依存してリスクを高く見積もる必要があるという問題も存在する。

クラウド事業者の多くが、いわゆる「マルチテナント」モデルをとっている。複数の異なるサービスや異なる利用者（のグループ）を同じ基盤の上でサポートする場合、個々のサービスや利用者に問題が発生した場合、ほかにも波及する可能性を考えておく必要がある。例えば、ある利用者のアカウントが盗まれた場合や、ある利用者が悪意を持った場合なども、その利用者の属するグループ以外のグループの情報やサービスは、これらの脅威から保護されなければならない。また、あるサービスの障害や混雑がシステム全体に波及しないような対策も必要だ。

しかし、これらは基本的な、認証・アクセス制御やリソースマネジメントの問題である。マルチテナントモデルにおいては、この問題をより緻密に考える必要があるというだけだ。同様に、例えば仮想化基盤の脆弱性、ローカルでの権限昇格脆弱性(*1)といったアクセス制御の根幹にかかわる問題は、よりリスクの高いものとして扱われなければならないだろう。インターネットを利用する、いわゆる「パブリッククラウド」の場合はさらに、認証システムが攻撃を受ける可能性や、サービス妨害の可能性などについても考えなくてはならない。前者はより強力な認証方式の導入で、後者はクラウドお得意の「スケーラビリティー」や物理的、論理的なロケーションの分散などが対策の要となるだろう。

サービス妨害のリスクという意味では、アクセス従量課金モデルをとるクラウドインフラ提供サービス固有の危険性も指摘されている。クラウド基盤を借りてサービスしている事業者に対して、アクセス集中を発生させ、課金負担を増大させるという攻撃だ。これは、EDoS（Economical Denial of Service）とも呼ばれるが、こうした可能性については、基盤提供側で、いわゆるDoS/DDoSに対する対策や攻撃を受けた利用者への経済面での救済策が用意されるべきだと思う。

### 求められる契約や法制度上の問題への対応

さて、こうして見ると、クラウド固有の技術的問題は意外と少ないように思える。実際、多くの利用者がクラウドの課題として挙げるポイントは、すでに大部分が技術的にはクリアになっている。

残る問題が、契約、制度（法制度）などの問題だ。例えば、機密保持契約において、預かった情報の保管場所を情報の所有者に明示する必要が記載されていたとす

る。こうした情報を、高度に仮想化され分散されたクラウド基盤に置くことは、契約違反のリスクを伴うことになる。こうしたシステムにおいては、データの物理的な所在が勝手に移動したり、特定できなくなったりする可能性が高いからだ。たとえ、そのクラウド基盤のセキュリティーがどれだけ高度であっても、この一点のみがリスクとなるのである。このような条項は、もともとクラウドのような考え方が発達する前にはよく見られた契約の内容だ。しかし、クラウドのような形態が想定されていなかったがゆえに、担保されるセキュリティーのレベルにかかわらず、クラウド化することだけで、契約違反とみなされるような条項が含まれているのである。これが、いわゆる「想定外」問題だ。

クラウドの時代であれば、この条項は、物理的なロケーションではなく、委託先の事業者が所有するファシリティーというような広義の意味合いで解釈されてもいいのだが、それには契約解釈上の合意が必要になる。委託先に対する実地監査を義務付けているような場合についても注意が必要だ。セキュリティーや内部統制に関する外部認証の取得により、個別監査が免除されるというのが妥当ではあるが、これも合意が必要だ。個別にこのような合意を得たり、契約条項を改定したりする労力はかなり大きな負担となる。多くの組織のセキュリティーポリシーや関連ルールも、（今となっては）レガシーなコンピューターシステムを前提に考えられており、多くの「想定外」が存在する。組織のルールはまだ変更が容易に思えるが、実際には先に述べたような契約や後述する法制度などとの関連で、改訂作業は簡単でないことも多い。組織とは独立した場で議論を行って、社会的なコンセンサスが得られるようなガイドラインを作り上げることが急務だろう。いくつかの制度上の問題さえ解決できれば、これは民間レベルでも可能な作業だと思う。

## 足並み揃わないクラウドのガイドライン

さらに大きなリスクとなりかねないのが、法制度の問題である。法律やそれに伴う政令、公的なガイドラインなどにも「想定外」の問題は存在する。これらは契約と同様に解釈による対応も可能だろうが、それには法律家の関与や所管する官公庁のお墨付きがいる。法制度については、それが現実に合わなくなりはじめてから動き始めるのが一般的だから、どうしても時間がかかる。

そして、それ以上に厄介なのが、国や地域による違いだ。インターネットをフルに活用したクラウドでは、データが国境を簡単に越えてしまう。従来のアウトソースでも、海外のデータセンターなどを使う場合に留意が必要なことはいくつかあった。安全保障上の輸出規制の問題(*2)や、相手国内の法制度による規制（例えば、犯罪捜査などの場合のデータ開示義務、個人情報の取り扱いに関する法制度の違い）といった問題である。クラウドの利用が一般化すると、データが国境をより頻繁に越えるようになり、こうした問題が一気にクローズアップされてくる。もちろん、ある国の中だけでデータを管理することは可能だし、現実に一部の事業者においても行われているようだ。しかし、そもそも大規模なクラウドサービス事業者が提供する安価かつ高いパフォーマンスの源泉のひとつが、複数のタイムゾーンへのサービスによる負荷ピークの平準化にあるのだから、それをタイムゾーンの限られた一国の国内、とりわけ日本のようなタイムゾーンが1個だけの国に限定することは、事業者にとっては大きな負担にもなる。もちろん、そのコストは利用者にもはねかえる。例えば、暗号技術の利用と適切な暗号鍵管理によって、情報の国外流出のリスクは許容可能なレベルに低下させられるのだが、それを代替策にするには、何らかの公的ガイドラインが必要だ。この問題の解決は、もはや一国では困難で、国際的な合意形成が必要となる。

残念ながら、世界的な政府間の枠組みで、制度問題を議論しようという動きは、まだ具体的にはみられない。しかし、すでに技術面では標準化の動きが始まっている。ISO（国際標準化機構）では、「分散アプリケーションプラットフォームおよびサービス」をテーマに「JTC1/SC38委員会」が立ち上がり、この中でクラウドコンピューティングが議論されることになっている。他の委員会でも、クラウドにからんだWG提案の動きが今後出てくるだろう。

国や地域のレベルでは、米国商務省管轄の標準化部局であるNIST（National Institute of Standards and Technology）は、クラウドコンピューティングの定義を定め、必要な検討作業に着手している。2009年10月に

公表された資料を見ると、クラウド利用のメリット、デメリットが整理されており、デメリットに対する対処策もいくつか提言されている。これは、当然ながら政府機関のクラウド利用もにらんでの話だ。

EUの情報セキュリティー部局であるENISA（European Network and Information Security Agency）でも、クラウドコンピューティングに関するリスクアセスメントを実施して、報告を作成しており、一読の価値がある。クラウドの震源地である米国もさることながら、意外なことにヨーロッパも真剣だ。ENISAの報告書では、クラウド利用のシナリオをいくつか想定した上でリスクを評価しているが、その結論部分では細かな推奨策が提示され、また、利用者側と事業者側の責任分界点を明記するなど、クラウドの浸透を前提に、それを安全に“使うための”ものとして書かれていることが読み取れる。これらの多くは技術的な面での動きではあるが、この後に来る制度面での交渉を有利に進めるための布石と見ることもできるだろう。興味深いのは、最も高いリスクと評価されたものの多くが、法制度面や、特定ベンダーの独自仕様に依存した「ベンダーロックイン」のリスクなど、非技術的なものであることだ。技術的なリスクは、中程度に評価されているものが多い。これは、制度面を重視するヨーロッパ的な見方ともいえる一方で、技術面に比べてこうした制度面の改革が遅れていることを示すものでもあるだろう。実際、報告書の最後の項では、EU委員会に対して法制度面での具体的な提案も見られるのが興味深い。

民間レベルでの動きも進んでいる。クラウドセキュリティーの普及を目的として、CSA（Cloud Security Alliance）が、現在、大手事業者やベンダーなども巻き込んで活動を行っている。CSAは、個人会員を主体に主な活動場所をSNSのLinkedIn上に置き、活発な議論を展開している。地域ごとのサブグループも続々と誕生しており、日本のサブグループも立ち上がって、2010年6月頃をメドに支部としての活動を始める方向で準備が進んでいる。

## 民間レベルの検討が加速する日本

日本でのクラウドに関する動きは、まだ多少混沌としているが、民間レベルではクラウド化を前提とした動きが徐々に見えはじめてきた。先に述べたCSAの日本支部（CSA Japan Chapter）設立の動きのほか、日本セキュリティ監査協会（JASA）が、クラウド利用を前提とした監査ガイドラインの策定作業を開始している。また、日本ネットワークセキュリティ協会（JNSA）では、英国に本拠を置き、欧米中心に活発な活動を行っているInternet Security Forum（ISF）と共同で、クラウドセキュリティーの研究を進めようとしている。どちらかといえば、当初はメーカーや通信事業者、データセンター事業者などによる基盤系の研究に偏っていた日本のクラウド関連の動きだが、ここにきて利用する立場から必要な事項の検討も加速し始めたようだ。インフラ面でも、大手ISPやデータセンター事業者を中心に、海外勢に対抗できるような、安価かつスケーラブルなクラウドコンピューティング基盤をサービスとして提供しようという動きが始まっている。こうした動きを加速していくことは、今後の日本が国際的な競争力を保っていくためには不可欠な動きだと思う。国際的な枠組みが決まってから動いたのでは、もう遅いのである。これは、日本のITにとっては大きな課題だろう。

クラウドの発展方向の予想は難しい。ただ、これが既存のパラダイムを足元から大きく揺さぶっていることだけは間違いなさそうだ。インターネットの普及期におけるISPの変遷と同じような状況が、クラウドの特にインフラに近い部分で繰り返されるような気がしてならない。そして、それらのインフラをいち早く上手に使ってビジネスを拡大したものが勝者となっていく。IT/ICTの世界は、またしてもひとつの大きな節目を迎えようとしているのかもしれない。

（＊1）脆弱性を悪用することで、システム管理権限でしかアクセスできないような機能やデータに一般の利用者がアクセスできてしまうような脆弱性をいう。あるユーザーが本来アクセスできないはずのほかのユーザーのデータを参照したり操作できたりする可能性があるため、特にマルチテナントのシステムにおいては危険度が高くなる

（＊2）日本では、ハイテク製品、関連情報などを国外に輸出する場合、経済産業省の許可が必要になる。こうした情報を国外にある自社拠点や委託先のコンピューターに保管する場合、そのシステム管理者などを含む海外在住者（海外在住であれば国籍を問わない）が内容を参照できる手段が存在する場合は、輸出とみなされる

参考サイト
- NIST（Cloud Computing Project） http://csrc.nist.gov/groups/SNS/cloud-computing/
- ENISA http://www.enisa.europa.eu/
- CSA http://www.cloudsecurityalliance.org/


# ［インターネット白書ARCHIVES］ご利用上の注意

このファイルは、株式会社インプレスR&Dが1996年～2012年までに発行したインターネットの年鑑『インターネット白書』の誌面をPDF化し、「インターネット白書ARCHIVES」として以下のウェブサイトで公開しているものです。

http://IWParchives.jp/

このファイルをご利用いただくにあたり、下記の注意事項を必ずお読みください。

- 記載されている内容（技術解説、データ、URL、名称など）は発行当時のものです。
- 収録されている内容は著作権法上の保護を受けています。著作権はそれぞれの記事の著作者（執筆者、写真・図の作成者、編集部など）が保持しています。
- 著作者から許諾が得られなかった著作物は掲載されていない場合があります。
- このファイルの内容を改変したり、商用目的として再利用したりすることはできません。あくまで個人や企業の非商用利用での閲覧、複製、送信に限られます。
- 収録されている内容を何らかの媒体に引用としてご利用される際は、出典として媒体名および年号、該当ページ番号、発行元（株式会社インプレスR&D）などの情報をご明記ください。
- オリジナルの発行時点では、株式会社インプレスR&D（初期は株式会社インプレス）と著作権者は内容が正確なものであるように最大限に努めましたが、すべての情報が完全に正確であることは保証できません。このファイルの内容に起因する直接的および間接的な損害に対して、一切の責任を負いません。お客様個人の責任においてご利用ください。

お問い合わせ先 | 株式会社インプレスR&D | ✉ iwp-info@impress.co.jp