

Tomura 式“クラウド・リーガル・クリニック”

～クラウドの法務的整理で

クラウドリテラシーを高めるために…～

日本マネジメント総合研究所 戸村 智憲

理事長／日本クラウドユーザー協会 会長

ここでは、戸村の私見として、クラウドに関する法的課題についてお悩みの声を寄せられた方々にお答えする形で、クラウドに関する誌上“リーガル・クリニック”として本稿をまとめてみた。

あくまでも、筆者は弁護士ではないため、法律相談というよりも、私見と展望をまとめたものとしてお読み頂きたい。

その一方で、クラウドに関し、国内大手法律事務所の弁護士の方々からクラウドと法務的観点についてのご相談・ご質問や指導を行わせて頂いてきた中で、クラウドと法務を考える上で本稿が何か読者諸氏のお役に立てるようなら幸甚だ。

“症例”①：個人情報保護法やセキュリティとクラウドの関係に悩み夜も寝られない

【カルテ】

クラウドに関する法務的対応に悩んで“不眠症”みたいになる方々が少なくない昨今であるが、クラウドに関してICTのガバナンスやセキュリティの対応をとる上で、既存のISMSやISO 27000系の対応でも契約のしか

た次第で十分な可能性もあるが、クラウド特有の問題を検討・対処していく上では、クラウドセキュリティアライアンスのガイドラインや業務委託先のICT環境もカバーし得るCOBITなどの方がよりクラウドに即していると筆者は考えている。

ただ、個人情報保護法について「クラウドだから危険だ」という議論には注意が必要だと筆者は感じている。

特に「クラウドでは個人情報管理が問題だ」と言われる方々の中には、セキュリティ上の不安をあおって、クラウドではなく従来のオンプレミスにおけるセキュリティツールを販売したいというICTベンダーや専門家の思惑が働いているケースがあるからだ。

日本の個人情報保護法は確かにクラウドを想定してできていない。したがって、日本の個人情報保護法においてクラウド活用した際の問題というのは、各個別の状況によってはさまざまに変化してくる可能性がある。

しかし、クラウドを使ったからといって問題があるというわけでもない。実際に、各企業で悩む以前に、経済産業省も山梨県庁などの自治体などにおいて、また、日本郵政やそ

の他の大手企業・行政機関などが、すでにクラウドを全面的に活用している。皆様が知らないところで、地方銀行などでも基幹システムをクラウドで運用しているようなところもある。

本当にここでクラウドに関する法的リスクを100%なくすというのであれば、Yahoo!やGoogleなどの検索エンジンを使えないことになってしまう。

実際にこれらの検索エンジンにおいては、アメリカにあるサーバーにおいて自然と検索者がどのような検索キーワードを用いたか、また、それに応じた広告を表示させるというシステムを使っている。

そのため、どのような方々がどのような検索ワードを用いて検索エンジンを利用しているかといったようなデータというのは、クラウドが流行し出す以前からすでにセキュリティ上の課題として検討すべき項目としてあがっている問題でもあったのである。

もちろん各企業のICTセキュリティ投資を何百億円かけても個人情報管理のリスクはゼロにはならないし、筆者が指摘してきているように「オンプレミスだから逆に安全である」ということも実態を見てくる中ではありえない議論である。

その観点では、クラウドと法務対応における落とし所として、Pマーク（プライバシーマーク）を取得しているクラウド提供企業やデータセンター、また、SLA（サービスレベルアグリーメント）で個人情報を保護できる契約事項を締結できるようにすることで、現状では一定の十分性を持った対応をとれるものと筆者は考えている。

また、海外のクラウド提供者に関して、海外にデータセンターやデータの拠点を置くこ



とが問題であると考えている企業も多いようだ。

しかし、個人情報を保護法に関しては、アメリカのセーフハーバー原則（自主規制を順守することを企業が自己宣言する）やEUのデータ保護指令などを見た場合、日本の個人情報保護法よりもはるかに高度で厳密な対応が余儀なくされている。

そういった観点からは、個人情報保護法とセキュリティやクラウドを見ていく中では、逆に日本の中にあるサーバーやデータセンターにデータを預けておくよりも、海外のクラウド拠点をを用いて米国のセーフハーバー原則やEUのデータ保護指令が及ぶ管轄内でデータを保管しているほうが安全であると見ることもできる可能性があるかと筆者は考えている。

“症例”②：クラウドが関わる法的側面に戸惑いが生じて動悸・息切れ感が止まらない

【カルテ】

現行法のすべてが必ずしもクラウドを視野に入れて制定されていない状況が、実際には日本の法体系の中にある。

なかには、はるか昔、明治や昭和の時代につくられた法令が今も厳然として、インター

ネットやクラウドを管理する関連法令として適用されている例すらあるのだ。

しかし、基本的には従来のインターネット法理が適用されるということは、国内の大手弁護士事務所の弁護士との情報交換や意見交換の中で見解を寄せてくれている。

クラウドの法律的な性格としては、主に次の3つの性格を帯びているというふうなことも考えられる。

- ① クラウドにおけるライセンス使用許諾
(ライセンス、バージョンアップなど)
- ② 設備・役務提供 (データセンター、運用・保守など)
- ③ カスタマイズにおける開発委託 (クラウド・インテグレーターなど)

上記のような重要3大ポイントの面において、日本の法が従来のインターネット法理の観点で適用されてくると、日本においては考えられる。

ただし、クラウドで海外のデータ拠点をを用いる場合の課題がないわけではない。準拠法や管轄法廷の問題があるのだ。アメリカの法理においては「ミニマム・アクセス」という観点がある。

つまり、アメリカの拠点とのやりとりでは、最低限何らかの関連がある、あるいは、何らかの仕事・連絡といったものがとられるところであれば、アメリカ国内での外資系のアメリカのクラウド提供者との訴訟となった場合、アメリカ国内の有利な管轄法廷に訴訟が持ち込まれる可能性がある。

そうすると、法廷での言語的なハンディもあるわけであるし、損害賠償額の通貨基準の問題も実際の法務実務として検討せざるをえない問題としてあがってくることになるだろう。

また、アメリカにおいては、州法によって、例えばカリフォルニア州やニューヨーク州などによって、法律上の判断が変わってくる可能性もあるため、当然、アメリカ在住の企業が訴訟を持ち込む、あるいは訴訟にされる場合に、クラウドサービスを利用する企業との間で合意された管轄法廷をクラウド提供者側にとって有利な管轄法廷に設定されるケースもあり、その点ではよく契約書などを検討しておく必要があるといえそうだ。

ただし、このようなことは従来のICTやICTを用いない取引においても同様のことであるので、「クラウドであるから管轄法廷や準拠法が問題である」とは必ずしも言い切れない。

逆に言えば、クラウドだからこれまでのインターネットを介した法的課題とは特殊で異質な問題があるというのは早計であるということは、念のため申し述べておく必要があると思われる。

“症例” ③：パトリオット法（米国愛国者法）に過剰に反応して歯がしみる“知覚過敏”

【カルテ】

クラウドというと、弁護士の方が鬼の首をとったかのように、米国愛国者法、いわゆる、パトリオット法というものが持ち出されがちである。

確かに何か有事の際には、米国当局が日本の企業のデータであろうと情報を閲覧することができるというような条項が法律で決められていることはご承知の通りである。

クラウドで機密情報や内部情報が「漏洩」あるいは「閲覧」されるという危機感が弁護士の方々がよく述べられることだが、パトリ

オット法は基本的にテロや戦争など有事の際の国防的な意味合いが強い面があることもご承知の通りであろう。

そのようなパトリオット法を論拠にクラウドは危険で使うべきでないとするならば、日本の国防になっているイージス艦やF35などの主力戦闘機となるものなどをアメリカから日本の国防として購入できないはずではないか。

例えば、イージス艦にせよ戦闘機にしても、アメリカから購入しているものに関しては、アメリカの戦闘機メーカーやイージス艦製造企業においてすべて図面や仕様や能力などが把握されているわけである。

その点を考えると、国際的な国防という私企業の商取引よりはるかに重大性の高い物事とは異なる個々の商業における観点の法律を扱う際に「クラウドはパトリオット法があるから危険だ」というのはあまりにも一般企業の用いるクラウドでの議論としては違和感があると筆者は感じている。

もちろん民間でも軍事的機密や国防関連データを扱う際には、確かにクラウド以前にインターネットなどから隔離したICT環境を用いると同時に、某メーカー企業が実際に某国のデータセンターに直接データを接続されるというようなウイルスソフトに感染するような事態があったが、クラウドを用いないまでもメールやこれまでオンプレミスで用いていたICT環境を用いることすらできなくなるというほどに過剰な対応が余儀なくされる可能性もありえるわけだ。

また、そのような標的型のサイバー攻撃に対処するため、むしろ、すでにICT大手企業ではクラウド化による集中防衛体制を敷いている。グループ企業全体のICTセキュリ

ティを、クラウド化により一元管理・高度化して、個々の部門に脆弱性を放置・潜在させることのないようにする動きが出ているのである。

そのようなことも考えると「パトリオット法があるからクラウドは使うべきではない」という議論はあまりにもクラウドに関してリスク過敏というか“知覚過敏”になりすぎているのではないかと筆者は感じている。

また、このパトリオット法が叫ばれる割には、オンプレミスであっても求められる「E-ディスカバリー」という制度に関して述べられることが少ないのが筆者として不思議でならない。

E-ディスカバリーは、従来どおりのオンプレミスの環境でも、アメリカ企業と法廷闘争になり、アメリカの法廷で争う場合に、機密情報などを含めて電子データを法廷に開示しなければならないということになっているものだ。

つまり、その場合、パトリオット法やクラウド利用が適用されない場合においても、アメリカとの訴訟ではE-ディスカバリー制度によって、当局あるいは裁判所等によって自社のデータがクラウドを使っていなくても閲覧されるという危険性があるという見方がされるわけだ。

そうすると、極論すれば、ICTセキュリティを高めるためにはアメリカと一切の取引をしてはならないというような結論、あるいは、自社の業務はすべてICTを用いてはならない、または、インターネットやメールを用いてはならないといったようなリスク過敏な対応に終始する可能性もあり得よう。

筆者としては、パトリオット法、また、E-ディスカバリーという観点からクラウドを

考えた場合にリスク過敏に陥る¹ことを避けるべきだと考える次第だ。

“症例”④：クラウドにおける独禁法に関するうつつとした“気分障害”

【カルテ】

独占禁止法について考えてみると、特に外資系の企業が日本でクラウドの隆盛を誇っている中で、確かに問題があるのではないかと筆者は考えている。

クラウド提供者側によるロックインが問題視される背景は何かといえば、大手クラウド間のデータ移行が事実上難しいという「スイッチングコスト」の高さが課題となっているということなのだ。

最初からクラウド利用する場合を除き、事実上、既存のオンプレミスのICT環境からクラウドへの移行に関しては「クラウド・インテグレーター」としての作業が必要となるケースがあり、「いったんクラウド化したものは、またオンプレミスに戻すということの後戻りがしにくいことも実例として生じてきている。

本来は、クラウド自体は使った分だけ使いたい分だけ使い、いつでもやめられる、またいつでもどのようなクラウドにも乗り換えられるようにしていくのが、開かれたICT環境、よりフリーな、より障壁の少ないICT環境の構築というクラウドの理念を実現する上で必要なはずである。

しかし、残念ながら、現在では必ずしも十分にその理念が生かされていないのが悔やまれてならない。

独占・寡占によって国内の企業がある特定のクラウドに「支配」されるという危機感もごもっともである。

しかし、すでにマイクロソフトのOfficeやSAP（ERP市場最大手のソフトウェア）などの従来からあるソフトやサーバーでは、オンプレミスの状態でとくに独占・寡占の障害を被っているわけで、オンプレミスの段階でもすでに独占禁止法についての問題が出ていることでもある。

したがって、「クラウドだから独占禁止法の問題が非常に避けるべき重大な課題である」という認識を持つのは果たして正しい議論かという点で筆者はそう考えてはいないのだ。

クラウドの黎明期～成長期における過渡期に、多少なりとも独禁法的な問題やクラウドの本来目指していくべき道からそれることはあろうが、その時期を超え、クラウド提供社との交渉力の強化や、外資主導で進んできたクラウドを国内独自クラウドの利用に転換するなどの対応などを含め、自社にとって良きクラウドを見出し活用する筆者の提唱した「クラウドリテラシー」を備えて頂きたいと願っている。

“症例”⑤：B to Cにおけるクラウドがもたらす涙目・鼻水・“花粉症”

【カルテ】

B to Cベースのクラウドの場合においては、消費者契約法について考えることができるであろう。

実際、クラウドと法務について研究を試みている法律学者の方や、一部のクラウドに多少は接している弁護士の方々によれば、少々マニアックに陥り勝ちともみられそうだが、クラウドに関わる法律に関しては120以上の法律が実際に関わってくると話してくれた。

そのすべてに関して見ていった場合には、実際に従来どおりのオンプレミスでも当然関

わってくる問題、あるいはインターネットというクラウド以前の問題に関しても関わってくる法律があげられているケースもあり、必ずしも「クラウドだから120を超える法律が問題である」という議論にはならないということには留意が必要だ。

B to Bの問題以上に、B to Cの場合は事業者と契約者間の情報格差や交渉力格差が大きく、またクラウドは特に規模の経済を生かす上で非常に消費者の力が弱い、契約者の力が弱いという傾向にある。

現行では、ある意味で「暴君」的な経営をしているような「乱雲」となるようなクラウドもあると言って過言ではない。その点では、クラウドを見極めるという視点が重要で、いかにクラウドリテラシーを備えていくかが、パーソナルクラウドが流行し始めた“花粉症”初期段階において、個人レベルでも求められている。

個人契約のクラウドやデータストレージなどでよく用いられているものに関しては、24時間前の告知でいきなりサービスを停止され、大事な写真や動画やデータなどが失われたという某大手ICT外資系企業の子会社の問題があった。

これなどはクラウドの手軽さによって爆発的に普及するがゆえに、より大きな消費者問題を導きかねないという観点はあり得るだろう。

国内においては、消費者と事業者間のすべての契約に適用されるものとして、消費者契約法で考えていくものとしては、契約の取り消しをできる例として、不実告知や断定的判断による情報提供、不利益事実の不告知などがあげられる。

また、契約を無効にできる例としては、事

業者の損害賠償責任を免除したり削減したりするような場合や、不当に高額な契約損料あるいはキャンセル料、不当に高額な遅延損害金や信義誠実の原則に反した消費者利益を一方的に害するような場合が当てはまる。

個人でもクラウドに関し、消費者の団体訴訟のようなものが起こされることや、個人レベルで消費者契約法を基にしたクラウド提供社への提訴など、暴君型クラウド提供社への対抗策というか、クラウドにアレルギー反応を示すよりも大切な涙目になって泣き寝入りをしてしないで済むように、ここで述べたような事前に検討しておくべき点を予防接種的に知識として備えておくことが求められよう。

“症例”⑥：「日本国内のICT＝絶対安全」と思い込み思考停止する“心肺停止”状態

【カルテ】

依然として、日本国内のICTが絶対安全、という思い込みや固定観念が暴走し過ぎて思考停止というか“心肺停止”的な状態に陥っている方々が多いように見受けられる。もちろん、日本のICT企業が提供するクラウドの方が、日本企業の商習慣やユーザビリティでかゆいところに手が届く良いサービスを展開してきているところは多い。

しかし、一歩踏み込んでみると、個人情報保護法関連に関してさらに考えてみた場合、この“心肺停止”的な状態には、心肺蘇生法と電気ショックで、クラウドリテラシーの観点から見つめ直すべき点として、以下のようなことが理解されておくべきだと筆者は考えている。

「日本の個人情報保護法は万全か」という問いかけをしてみれば、クラウドを視野に法

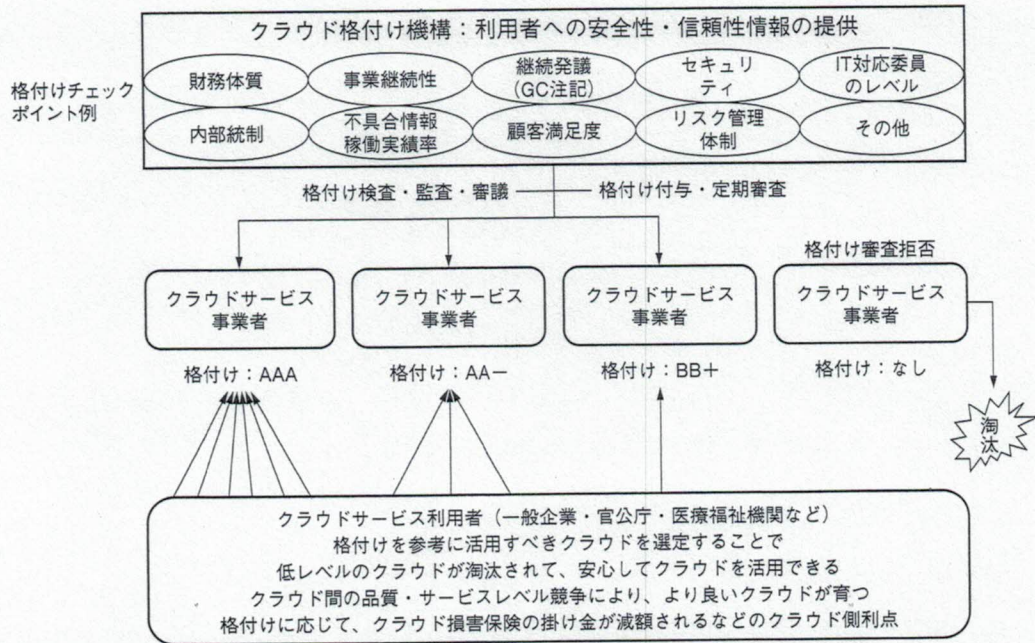


図1

律が制定されていないため、国際間でのデータトランザクションに問題が生じる可能性があり得る。

また、EUのデータ保護指令やアメリカのセーフハーバー原則などと日本の個人情報保護法が同等性評価を得ていないため、日本の個人情報保護法は国際的に見れば海外の企業が日本のデータセンターなどにデータを預ける方が、国際的視野からすればよりリスクであるというような国際間の実態があるわけだ。

むしろ、EUやアメリカのほうが個人情報保護に関してはデータ保護の面でも進んでいるということもできる。

「アメリカに日本から個人情報を持ち出す危険性」よりも、「アメリカやEUなどから日本に個人情報を持ち出す」ほうが危険だと見られているようなもので、言ってみれば日本企業の被害者意識が高いというように筆者は見ている。

日本の個人情報保護法も、EUのデータ保護指令やアメリカのセーフハーバー原則と同等性評価を得られるように改定が急務であると筆者は考えている。

したがって、「日本国内＝安全」という前提や思い込みでの議論は、クラウドにおけるフェアな論議にはなっていないと筆者は考えている次第だ。

“症例”⑦：このままこのクラウドでいいのか？と悩む不安に襲われる“パニック障害”

【カルテ】

中には、すでにクラウド化を進めている企業の方が、「このままこのクラウドでいいのか」「このクラウド提供社が倒産や買収などされたらどうしよう」と、突如、不安に襲われ、言ってみれば“パニック障害”的な心理にかられる方々がいるようだ。

そこで、ここでは少しクラウド・ベンダー

の倒産や買収、M&A などについて考えてみることにしよう。

クラウドは「雲」というように言われるように、実際にある「雲」が消滅して、雲散霧消してしまうということもあるといえはるわけだ。

クラウド選定をする際に、ICT 面や ICT 面以外での取引と同様に、事業の継続性や監査、財務報告における「継続疑義」などにも留意しておく必要がある。

末永く「温暖湿潤な気候」や「雨」をもたらす「雲」なのか、最大瞬間風速だけはすごそうな「積乱雲」かを見分けるための仕組みが必要になってくるのだ。

その点で筆者はすでに書籍の中で「クラウド格付け、クラウド与信などの仕組みが必要である」という提言をしてきた(図1参照: 出典は拙著『なぜクラウドコンピューティングが内部統制を楽にするのか』(技術評論社))。

このようなクラウドに関する与信や格付けに関する仕組みが業界標準的に整うまでは、自社で取引基準を設けておく必要がある。それは ICT 以外の取引においても同じように適用される与信管理のようなものだ。

万が一のため、あるクラウドを別のクラウドでバックアップするような、クラウドをクラウドでバックアップする、あるいは、クラウドをクラウドで統制する(クラウド統制)といった対応も必要になってくる。

また、ある小さな「雲」が大きな「雲」や「暗雲」に飲み込まれてくっつくというような M&A も考えられる。

「クラウド内部のファイアー・ウォールがあれば、買収されても競合企業と同じクラウドを用いても問題はないのではないか」という、日本の大手弁護士事務所の有力な弁護士の方々からご相談をお寄せ頂いたが、筆者はそのとおりであると考えている。

暗雲となるクラウドとくっついたら、場合によっては、その際はクラウド乗り換えを検討することやクラウドの契約を解除することも必要になってくると筆者は考えている。

クラウド化においても、既存のクラウドに対するリスク管理策や既存クラウドの事業継続性の観点から、クラウド間移行の可否やその際のコストなどの検討を、あらかじめ行っておく方が安心であろう。

まとめ

以上のように、クラウドと法務的側面を筆者の私見と展望という形で誌上クラウド・リーガル・クリニックとしてまとめてみた。

読者諸氏において、ここで述べたことへの異論反論は大歓迎であるし、新たに異なるご質問やお悩みなどがあれば、筆者に忌憚なきご意見・ご感想をお寄せ頂きたい。

(HP: <http://www.jmri.jp>, E-mail: info@jmri.jp)

ユーザーのための
ソリューションガイド

ITソリューション

企業総覧

2012年度版

ICT×ビジネス

特集

激変する経営潮流
～スマホ時代のICT環境づくり

巻頭鼎談

場所に縛られないICT環境づくり
～激変する経営潮流をどう乗り切るか？

日刊工業出版プロダクション・編
日刊工業新聞社