最新・クラウドにおける「7つの法務的考察」

日本マネジメント総合研究所　戸村　智憲
www.jmri.jp/
理事長

ファーストサーバ社のデータ消失問題や、スマホのアプリでもPC上でも用いられるクラウドにおけるデータ保管サービスやメールサービスでのデータやパスワード等の漏えい問題があるからといって、果たして、「クラウド＝危険」という感情的判断によるレッテルをクラウドに張り付けても良いのだろうか。

また、クラウドを危険視する根拠として、これまでは弁護士の方々が米国パトリオット法を持ち出すものの、その他の法的な対応にはどのようなものがあり、「クラウド＝危険」と結論付けるに論理的妥当性があるものなのだろうか。

筆者は弁護士ではないので、法律相談というお話しではないが、各大手弁護士事務所の弁護士の方に筆者が講演やディスカッションをする中で、筆者の私見的にクラウドに関わる法務的側面についての7つの法務的考察を本稿にまとめておこうと思う。拙稿が、何か少しでもクラウドと法務対応における参考になれば幸いだ。

【法務的考察・その1】個人情報保護法やセキュリティーとクラウド

クラウドに関してITのガバナンスやセキュリティーの対応をとる上で、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ーアライアンスのガイドラインや業務委託先のIT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、セキュリティー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ーツールを販売したいというIT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るとはいいがたい。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。実際に既に実績として経済産業省も山梨県庁などにおいても、また、日本郵政やその他の大手企業・行政機関などが既にクラウドを全面的に活用しているし、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のだ。

本当にここで100％リスクを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、アメリカなど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ようなシステムを使っているため、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既にセキュリティー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る。

もちろん、各企業のITセキュリティー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、これまで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必ずしも妥当ではない議論だと筆者は思っている。

その観点では、落とし所としてＰマーク（プライバシーマーク：JIPDECにより個人情報保護の体制を整備している事業者を認定した登録商標）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、現状ではある程度十分な対応をとるしかないのではないか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が、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ー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と筆者は考えている。

個人情報保護法関連に関してさらに考えてみると、このようなことが言えるのではないかと筆者は思っている。

「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ると、クラウドを視野に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のだ。

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ほうがよりリスキー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考え得るわけである。

「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次第だ。

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な改定が急務である。

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。

【法務的考察・その2】
クラウドと法務全般

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。

中には、はるか昔、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がある。

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た。

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）

といった面において、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キャップ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、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ITやIT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ということは、申し述べておく必要があると思っている。

【法務的考察・その3】クラウドとパトリオット法(“米国愛国者法”)

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を持ち出される。

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。

クラウドで機密情報や内部情報が「漏洩」あるいは「閲覧」されるということは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のである。

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、日本の国防を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のだ。

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IT環境を用いると同時に、某メーカー企業が実際に中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ようだが、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IT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。

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のだ。

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。

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のだ。

そうすると、極論すれば、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IT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えるので、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ことを避けるべきだと考える次第だ。

ちなみに、米国でのアップルv.s.サムスンの特許訴訟におけるE-ディスカバリーについては、訴訟で争う当事者が、自分にとって不利な証拠となるものであっても、訴訟の内容に関連性のあるデータ類であれば、法廷・陪審員・相手方に電子記録をすべて提出・開示しなければならないものとして、訴訟で相手方に対し、電子記録や各種データ類を合理的に考えて使用可能な形式・状態で開示・コピー・閲覧させることができる状態であった。

訴訟で相手方に提出形式なども特定・指定することができるし、特に指定なしの場合は通常の保存形式や合理的に考えて使用可能な状態で提出・開示することが必要（印刷・ファイルなど）となっていた。

この電子記録・データ類は、PC内やサーバ内のデータだけでなく、スマホ内のデータやデジカメやその他のあらゆる電子記録・データ類が、データ検索可能な状態で提出する必要に迫られるのである。

そして、「リティゲーション・ホールド」（Litigation Hold）といって、訴訟が起こると予測された時点で、有利／不利に関わらず、自社の関連データ・文書類の全てを保存する義務があり、非開示・非協力に対しては、陪審員に「不利な推定」をするよう指示される・有利な証拠の不採用などの制裁が科せられるものである。

訴訟において、サムスンがアップルとの訴訟に関連性のある電子データ類を保管すべき義務を意図的に無視したと認定されたこともあった。リティゲーション・ホールドを指示し、電子メールや各種データを削除しないよう2,700名以上の関係する従業員に周知徹底しなかった（14日間で自動削除される電子メール処理を削除停止にしなかった＆過去に違反処罰を受けていたにも関わらず再発させ、最初は20数名にしか通知していなかったなどの問題があった）。

ここで、サムスンは、従業員がリティゲーション・ホールドを遵守しているかチェックを怠った（E-ディスカバリーの管理体制不備が指摘された）ため、法廷で陪審員に対し、サムスンが不利な情報をかくしたものとして「不利な推定」をするよう指示される状態に置かれたようである。

ただ、実際にはアップル側のデータ保存対象に電子メールが含まれていなかったミスがあり、双方とも「不利な推定」をされないよう争点から外す旨の合意をしたという、ある弁護士いわく、「サムスンがE-ディスカバリーでの致命的なミスを、アップル側のミスに乗じてうまく逃げた」という状態であったようだ。

【法務的考察・その4】
独占禁止法関連とクラウドについて

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である。

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IT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あり得るのだ。

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IT環境、よりフリーな、より障壁の少ないIT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だが、残念ながら、今現在では必ずしも十分にその理念が生かされていないようで残念だ。

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はごもっともなことである。しかし、既にマイクロソフトのOfficeやSAP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っくに独占・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既に独占禁止法にかかわりそうな状況が出てきていることは明確なことである。

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、クラウドにおけるフェアな議論かというと筆者はそう考えてはいないのである。

【法務的考察・その5】
クラウドとB to Cの法務について

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も必要であろう。

実際、クラウドと法務について研究されている法律学者の方や、一部のクラウドに多少は詳しい弁護士の方々によると、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いうようなことも言われている。

しかし、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る。必ずしも「クラウドだから120を超える法律が問題である」わけではなく、あたかもクラウド固有の法令対応があまりにも仔細におよび現状ではクラウドを利用しない方が賢いという選択を誘発しかねないような議論が妥当だとはいえないのではないと筆者は考えている次第だ。

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のは問題だ。

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散見される。その点では、クラウドを見極めるという視点が重要だ。

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IT外資系企業の子会社の問題があったのは報道の通りである。

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えそうである。

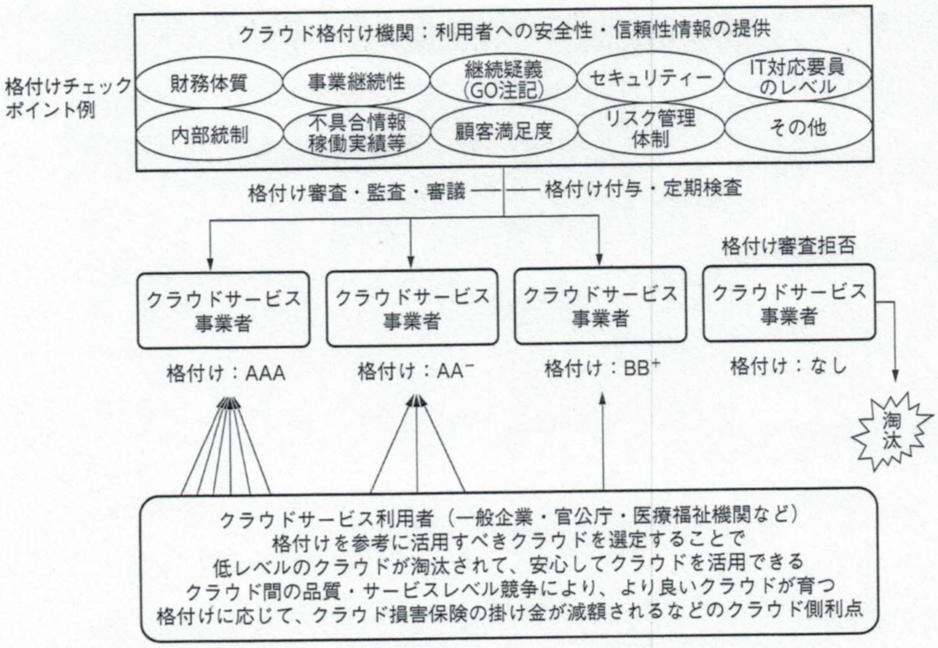

図1

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は、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のであろう。

【法務的考察・その6】クラウド利用環境における救済制度のあるべき姿

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たらどうであろうか。

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ばあるわけだ。

クラウド選定をする際に、IT面やIT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のだ。

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である。

その点で筆者は既に書籍の中で「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）。

この仕組みが整うまでは、自社で取引基準を設けておく必要があろう。それはIT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が…。

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、既に述べた、

クラウドがクラウドを統制するような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いても問題はない」という、日本の大手弁護士事務所の有力な弁護士の方々の見解と筆者は同意見だ。

暗雲となるクラウドとくっつくなら、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。

【法務的考察・その7】クラウドと契約・SLA（サービスレベルアグリーメント）

クラウドと法務のその他いろいろな面に関して少し整理してみると、このようなことがあるのではないだろうか。

海外現地の各種業法に関して見れば、ITのみならず、多国籍にまたがる際の避けられない課題である。

準拠法と管轄裁判所をどこにするかやどこになるかといったことを明確に把握しておく必要がある。

また、自社にとってより有利な準拠法、より有利な合意管轄裁判所を、契約において締結しておくことによってある程度のリスクヘッジができると筆者は考えている。

不正競争防止法関連においては、営業上の機密保持における問題として、通常の機密保持契約とその違反事案における対処を契約において規定しておく必要があるということも考えうるポイントである。

契約内容での問題としては、サーバーダウンによる機会損失はクラウドだけではなくてオンプレミスにおいても生じているし、自社のサーバーのほうが意外といい加減であったりする企業も多いのではないだろうか。

契約書面の中でサービスレベルアグリーメントの合意内容として責任を明確化しておく必要があるだろう。

また、誤作動に関しては、IT環境では避けられないものの、どのような誤作動に対してどのような損害や問題にどう対処するかということを、クラウドを利用する際の契約書にて明確にするとともに、契約事項をSLAの観点からも結んでおく必要があると筆者は考えている。

☆　☆

このように、あくまでも筆者の私見として、法律とクラウドを改めて見つめ直してみたが、何かご意見・ご感想・異論反論・ご質問やご相談などがあれば、ぜひ筆者にご連絡頂きたい。

（日本マネジメント総合研究所 理事長 戸村智憲あて：メールはこちらから info@jmri.jp、ホームページからはこちらから http://www.jmri.jp/）

参考・引用文献

1）戸村智憲：危機管理型クラウド：場所に縛られないIT環境による危機に強く人にやさしい経営へ（税務経理協会）
2）戸村智憲：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）
3）戸村智憲：監査マネジメント技法（中央経済社）

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

2013年度版

特集｜ITが本当に日本を救うのか

巻頭対談｜危機的な日本のIT産業への提言

緊急鼎談｜ITに安易に「信頼」を求めすぎではないか？

日刊工業出版プロダクション・編
日刊工業新聞社