SOFTIC賛助会員セミナー〈第10回〉

―クラウド特集―

「クラウドコンピューティングサービスの提供に関わる問題点」

講師：弁護士　上沼紫野氏

目　次

＊本講演録は、当日の講演に講師が加筆・修正したものです。

平成２４（２０１２）年5月２２日

１８時～１９時３０分

於　SOFTIC会議室

○上沼　それでは始めさせていただきます。

今日参加されている皆様方はメーカーの方が割と多いので、サービス内容自体についてはよくご存じの方ばかりなんだと思いますが、本日の内容は、ユーザー向けを念頭にしているようなところもあるので、ユーザーとしてはこんなことを考えているのか、というような感覚で聞いていただければと思います。

本日は、まずクラウドがなぜ今そんなに話題になっているのか、従来と何が違うのか、ということと、情報処理の高度化に係る刑法の改正に伴ってデータ差押えの規定ができましたので、その話をちょっとさせていただきます。そのあとは、現在のいわゆるクラウドサービス特有の問題点は何かということを説明して、おまけで、クラウドと親和性が高いと言われているスマートフォンの問題について、ちょっとお話をさせていただければと思っています。

【１．　クラウドサービスに対するニーズ】

クラウドについてに一番感じるのは、クラウドサービスという言葉自体に対する各自の理解が違うというところです。

「クラウド」という言葉はバズワードのように使われていて、クラウドサービスという言葉自体が何を指しているのかがよく分からなくなっているために、例えばユーザー側とサービス提供者側で話が通じない、というようなことが実際に起こっているというふうに感じます。

この点を考えると、実際は「クラウド」ではなくて、具体的なサービス内容に基づいて議論をしないと、ユーザーと事業者の間で話が通じないのではないかと思っています。ちなみに、「クラウド」とはいつごろから使われ出したのかと思って検索をしてみたら、グーグル社CEOのEric Schmidt氏が2006年ぐらいに使ったもののようでした。この「クラウド」という言葉は、オラクルのＣＥＯ、Larry Ellisonが「クラウド」は新しいものを追求するコンピュータ業界が既に存在している機能を全て含めるものとして使っていると述べていることから、もともと多義的な意味で使われ出した言葉なのではないかと思っています。

クラウドの定義については、来週の岩原先生がされると思いますけれども、クラウドの定義としては、ＮＩＳＴの定義がよく使われているのかなというふうには思っていますが、ＮＩＳＴの定義からも特定のサービスが導かれるのではなく、最大公約数的なものを引き出して作られた定義のようですから、やなり多義的という部分は同じなのではないかと思っています。

では、なぜ、今、クラウドが流行っているのか、ということですが、基本的にはアウトソー

シング化の傾向があると思います。最近は、様々な側面でアウトソーシングが進められていていると思います。例えば、自社開発をすると費用がかかるから、外注によってコストを下げる、あるいは自社開発だと時間がかかるが、専門業者に依頼すれば、早くできるということで時間が短縮できるというニーズがあるのだと思います。又は、情報システム基盤を統一化したいということもあろうかと思います。各社が独自に開発すると、システムがその１社固有のものになってしまうわけですけれども、他のサービスを利用することで統一化することが容易になります。また、資産のオフバランス化の要請により、固定資産をなるべく自分で保有しない方向というのもあります。これらがクラウド利用のニーズなのだと思いますが、それに加えて、2011年の３月以降は、震災などに備えたデータの分散化の要請もありますし、環境的にはCO_2の削減に資するなどということもニーズとしてあげられていると思います。

【２．　従来から存在するサービスとの差異】

クラウドに関する問題点や議論をいろいろ聞いていますと、従来のサービスでも既に問題になっていた部分があると思います。

クラウドという言葉が一般化する前に、ファイル・ストレージサービスというのはありましたし、オンラインアプリケーションとしてネット上でアプリケーションを使うというサービスや、データベースをオンラインで使うというサービスもあったわけです。これらに存在していた問題点は、クラウドが一般化して初めて認識されたものではなくて、既にあった問題がまた改めて検討される、あるいはフォーカスされているにすぎないわけです。

従来から既に存在していた問題というものの例としては以下のようなものがあると思います。例えば、予定されていた機能が発揮できない、又はデータが喪失したというような事業者側のサービスの内容そのものに関する問題は、従来から生じていた問題です。また、ユーザーの著作権侵害等の行為について事業者が責任を問われる間接侵害も、そもそも「MYUTA」のころから問題になっていたわけで、これも「クラウド」が一般化したことによって初めて生じた問題点ではありません（間接侵害については、来週の岩原先生のほうで詳しくされると思います）。

また、不正アクセス等のセキュリティの問題は、インターネットを使う以上は付随する問題ですし、ユーザーの蔵置したデータの差押えの問題なども、従来あったファイルサーバなどでも存在していた問題だと思います。

今日は、クラウドに関し、従来から存在している問題というより寧ろ「今」のクラウドで特

に検討すべき点を中心にお話をさせていただきたいと思っています。

今のクラウドで特に重要な問題は、まずは、クロスボーダーに関するものではないかと思っています。特に今は、サービス提供事業者がグローバル企業ということもよくありますが、そのような場合は、サービス提供事業者自体が多数の国でサービスを提供し、資産を保有しているので、ユーザーとしてはサービス提供事業者のサーバーがどこにあるかわからない、ということがあり得ます。その結果、ユーザーからはデータ所在地がわからないということになりますし、クロスボーダーである以上は、準拠法や国際裁判管轄が当然のことながら問題となることになります。

また責任分担の問題も今のクラウドでは重視されることだと思います。クラウドでは、サービスの提供が多重構造になっている、つまり、いろいろな事業者が関与してくることがよくあります。例えば、プラットホームを提供しているクラウド事業者があって、その上で別の事業者がアプリケーションを提供し、また、ネット接続は別の事業者が提供しているということはよくあることなので、ユーザーの認識としては１つのサービスを契約したつもりであっても、実際に関与する事業者が多数存在するということになります。この場合、何か問題が生じたときに、どこの誰に対して何が言えるのかが、ユーザーからはわかりにくくなってしまいます。

あとはセキュリティの問題もあると思います。先ほど申し上げたように、セキュリティの問題は従来から存在していたものではありますが、クラウドについて、ユーザーが特に心配な点として挙げているものですので、クラウド特有のものとして取り上げさせていただいています。

【３．データ差押えに関する問題】

ユーザーの蔵置したデータに関する差押えの問題というのは、クラウドが一般化する前から存在していたものではあるのですが、改正法の関係でこのあたりの手続が変わろうとしていますので、特にお話をさせていただきます。

2011年の６月17日に「情報処理の高度化等に対処するための刑法等の一部を改正する法律」というのが成立しました。同法には、例のウイルス作成罪に関する改正もふくまれておりまして、こちらについては既に施行になっているわけですけれども、この手続に関する部分は本日現在まだ施行日が決まっていません[1]。この法律は、日本がサイバー犯罪条約に署名をしたことが経緯となっています。

[1] 2012 年６月 22 日施行された。

サイバー犯罪条約は2001年に欧州評議会で発案されたものですが、オンライン上の児童ポルノの規制や、不正アクセスの禁止など、いわゆるサイバー犯罪に関する規定が盛り込まれています。日本はこれに署名したものの、批准をするために一定の法律改正が必要な状況になっていまして[2]、これに関する法律の改正案が何度も国会に提出されていたのですが、この改正案にいわゆる「共謀罪」の新設が含まれていたため、反対も根強く廃案になることを繰り返していました。今回、共謀罪に関する規定を抜きにして成立したのが、この「情報処理の高度化等に対処するための刑法等の一部を改正する法律」です。

改正法では、ウイルス作成罪、インターネットがからんだ犯罪についての捜査等の手続の直しの問題などが扱われていたのですが、本法案の閣議決定がたまたま３月11日であったということもあって、ネット監視法案をどさくさにまぎれて成立させたという誤解が一部の人たちを中心になされていました。捜査手続きに関して、捜査機関がデータの保全を要請できるというような規定が入っていたことが、令状なしにデータの差押えができるというように誤解されて、ネット監視法案だと言われてしまったということのようです。

具体的な法律の内容は、法務省のホームページを見ていただければわかります。改正法に含まれる具体的な内容が図解で示されているほか、ウイルス作成罪に関して、Ｑ＆Ａなども充実していますので、こちらをご覧いただければ大変参考になると思います。

クラウドとの絡みでは、刑事訴訟法の改正が重要な点です。主な内容は、①接続サーバー保管の自己作成データ等の差押えの導入、②記録命令付差押えの新設、③データに関する記録媒体の差押えの執行方法の整理、また、④データの没収に関する規定の整備でしょうか。

上記改正は、サーバー等をネットを介して使っている場合を想定してなされたものではあるのですが、サイバー犯罪条約自体は2004年の発効です。それから今まで随分経ってしまったものですから、今の現状に必ずしも十分には対応しきれていない部分があって、この件で国会に参考人として呼ばれた指宿先生が、今回の改正ではクラウドの利用環境に十分対応しているとは言えない、というようなことをおっしゃっています。その理由として、例えば、データの所在地が不明である点を挙げています。データの所在地が不明だと、どの国の法律を適用すべきかがわからない、ということを国会で述べていらっしゃいます。

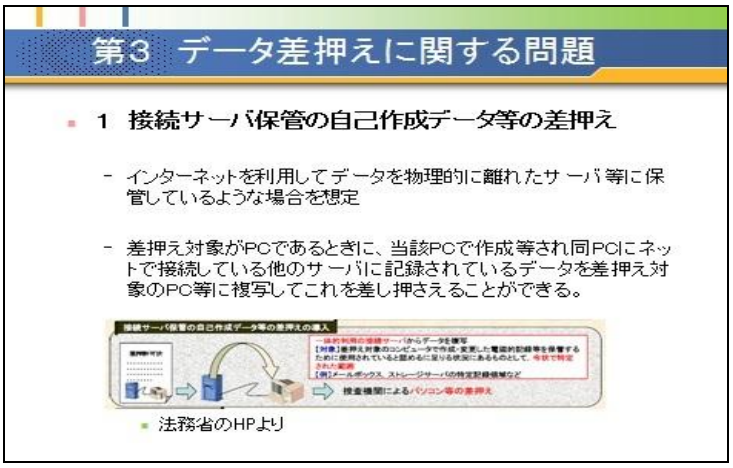
具体的な改正の内容について、まず接続サーバー保管の自己作成データ等の差押えについてお話しします。これは、インターネットを利用してデータを物理的に離れたサーバー等に保管しているような場合を想定しています。ファイルサーバーを使っている場合や、メールがサー

[2] サイバー犯罪条約は、日本に関して 2012 年 11 月 1 日に発効する。

バーにはあるが自分のローカルの端末には落としていないような場合を想定しています。

パソコンを差押え対象にするときに、そのパソコンで作成した、そのパソコンにネットで接続している他のサーバーに記録されているデータを、その差押え対象のパソコンに複写して、これを差し押さえることができる、というものです。　ローカルのパソコンが空っぽのときに、その空のパソコンを押さえてもしようがないわけで、サーバーのほうからローカルのパソコンにコピーして、差し押さえることができるということですね。

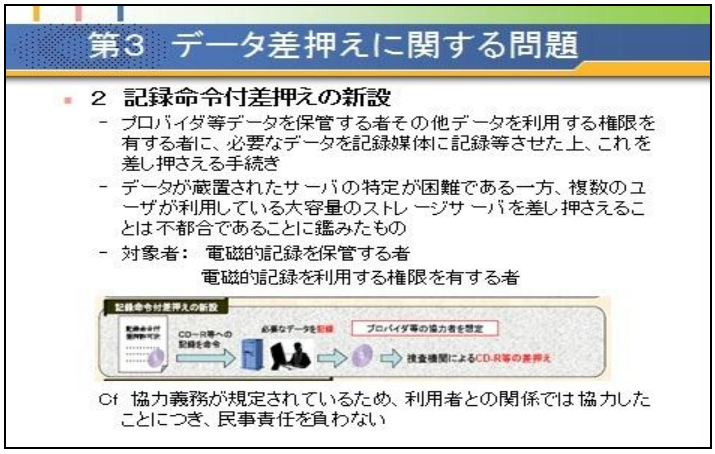
＜スライド9＞



上記は先ほどお話しした法務省のホームページにあった図です。どういうデータがその複写の対象とできるかについては、令状で特定された範囲ということにはなっていますが、具体的にはどんな感じの令状になるのかについては、施行されてから明らかになってくると思われます。

これとは別に、記録命令付差押えというタイプの差押えの方法も規定されています。

＜スライド10＞



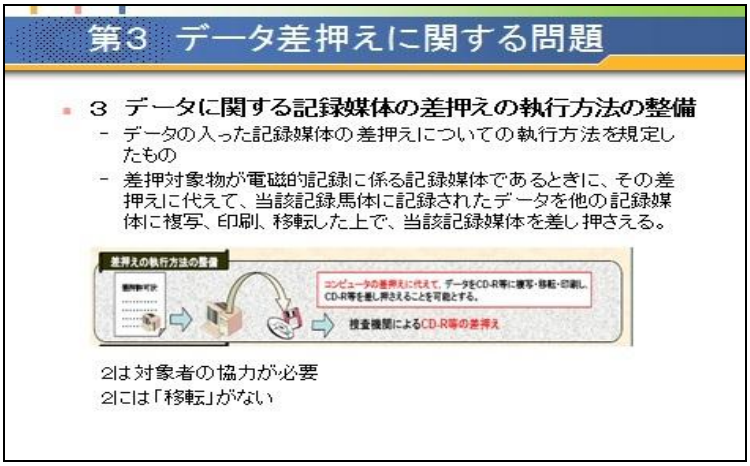
これは、プロバイダー等の、データを保管する者その他データを利用する権限を有する者に、必要なデータを記録媒体に記録等をさせた上、これを差し押さえるという手続です。ちょっと分かりにくいので、もう少し説明しますと、サーバーのどの部分に必要なデータが入っている

かは捜査機関から見てもすぐには分かりません。といって、サーバーごと差し押さえて持っていってしまうということになると、そのようなサーバーを複数のユーザーが利用している場合に、他のユーザーは、多大な迷惑を被ることになります。だったら、そんなことをしなくても、必要な部分のデータだけ記録して持ってくるということができればいいのではないか、ということで、必要なデータのみを、ＣＤ－ＲあるいはＵＳＢメモリーなどの記録媒体に記録させて、これを差し押さえることが可能とする手続きを作ったわけです。対象者は、電磁的記録を保管する者、あるいは電磁的記録を利用する権限を有する者となっていますから、クラウドサービスを提供する事業者は、この差押え命令の対象になり得ます。

本手続きは、もともと協力者が想定されていまして、プロバイダーやサービス事業者などによる捜査機関への協力によって本手続きが進むことになるのですが、してつくっている手続ですから、基本的には協力をしてくださいねという話になるんですが、プロバイダーとしては、捜査機関に協力した結果、ユーザーから損害賠償等を請求される結果になっては協力などはできません。そこで、法律で協力義務が規定されており、利用者との関係では捜査機関への協力を行ったことについては民事責任を負わないという構造になっており、これにより、差押えの実効性を担保しようとしています。

記録命令付差押えは、協力が前提になっていますが、協力が前提とされていない手続きもあります。データに関する記録媒体の差押えの執行方法の整備が、それに当たります。

＜スライド11＞



今までは、データの入った記録媒体の差押えについての執行方法というのが明確に規定されていませんでした。そのために、一部のデータが必要な場合にそれが蔵置されているコンピューターを丸ごと持っていくなどという形になっていたわけです。

基本的に、差押え等に関しては、法律が有体物を前提としていて、データを差し押さえると

いう発想がないものですから、無形物である「データ」を差し押さえるということはできませんでした。今回の改正でも、記録媒体という形で、差押えの対象は有体物であるという概念は維持されているのですが、記録媒体に記録されたデータを他の記録媒体に複写、印刷、移転した上で、その記録媒体を差し押さえるということができるとしたもので、事実上は、データそのものに着目し、これを捜査機関が入手する方法を整備したものです。つまり、コンピューターの中に入っているデータの一部を、別の媒体に移して持っていくというものですね。

記録命令付差押えの場合には対象者の協力が必要なので、データ保管者等が協力してくれないと実行できないのですが、こちらの手続きは協力がなくてもできるという点が相違点です。また、記録命令付差押えには移転という手続がありませんが、こちらにはありますので、この点も相違となります。

この「移転」というのは、刑事訴訟法ではもとのデータを消してしまうとことを想定しています。「複写」はまさにコピーであり、もとのデータはそのままなのですが、「移転」の場合には元のデータを消してしまって、新しいデータだけを残すことになります。

データの没収に関する規定の整備というのも、有体物を前提とした「没収」という手続きをデータという特性に合わせた整備を行ったものです。「没収」は有体物を前提としていたため、不正なデータが存在しており、これを使わせないという必要性があるときに、それを消すという手続が整備されていなかったため、これに対応した規定になります。

差押えのときに「複写」ではなくて「移転」を選択すると、もとの媒体上のデータが消えますが、データの入った記録媒体を還付しなくちゃいけないような場合にそのまま還付してしまうとデータも戻ってしまいます。そこで、そのデータを消去、あるいは不正に利用されないようにする処分を行うという条項が追加されたのですね。ウイルスなどのデータの場合、そのまま残しておくのは妥当ではありませんので、該当データを消去するということが必要になります。そのような場合に、まず「移転」とした上で、「没収」をすると、ウィルスデータが消えるあるいは使われることがなくなるということになるわけですね。

ほかにも細かい規定はありますが、クラウドサービス事業者が関係しそうな手続きというのは概ね今申し上げたところだと思います。

他には、捜査機関が、アクセスログをすぐに消さないで欲しいとお願いできるという手続があります。これはあくまでもお願いベースであり、これ自体では差押えではないのですが、この辺が誤解されて、ネット監視法だと言われてしまったのだと思います。

アクセスログの保全要請期間も60日を最大限度とするとなっていますから、データ保管者側

にとってもそれほど無理な内容にはなっていないと思われます。具体的には、まず、警察から「残しておいて欲しい」という要請が来て、その後、捜索差押え令状によって、先ほどの刑事訴訟法の差押え手続に進んでいくというような流れになります。

【４．クラウドコンピューティングに関する諸問題】

（１）サービス利用契約に関して

では、今のクラウドに関する問題点について説明させていただきます。先ほど申し上げたとおりクラウドのサービスは、多重構造となっているので、ユーザーからは誰にどのような責任が追及できるのか分からないということになるのは困ります。これに対する解決策は、実際には多分１つしかなくて、契約で、事業者が負うべき責任の内容を明確化してもらうということになろうかと思います。

今行われている債権法改正の議論とも関係してくると思うのですが、現行法の解釈では債務不履行については、債務不履行責任を問うためには相手方に帰責事由が必要だと解されているため、例えば多数の人が関与していた場合に、契約当事者ではない関与者の行為により問題の結果が生じた場合に、契約当事者にその責任を追及するためには、関与者を契約当事者の履行補助者とするなどの方法で、当該関与者の行為についても相手方が責任を負うべきだとするための根拠を検討する必要があります。一方、今の債権法改正では、債務不履行責任に帰責事由は不要という考え方をとろうとしています。つまり、約束したことができなかったこと自体は不履行であると解釈されることになります。

このような考え方を前提とすると、多数の関与者がいたとしても、契約内で、提供されるべきサービスの内容がきちんと明確化されていれば、その規定どおりのサービスが提供されなければ債務不履行だといえることになります。したがって、多数の関与者がいたとしても、契約相手に対して債務不履行責任を追及することは容易になると考えます。

ただ、契約で解決する場合の問題点は、利用者側に選択の余地が残されているか、という点です。というのは、結局契約にどう書いてあるかが全てという話になってくるので、ユーザーとしては自分の希望するサービスの内容が、契約内に過不足なく規定されている必要があることになりますが、そのためには、ユーザー側に十分な知識とバーゲニングパワーがあって、契約の条項に関する交渉がきちんとできることが前提になります。ところが、実際には、ユーザーがそこまでの知識等を有するというのはなかなか難しく、サービス提供者側が準備したメニ

ューの中からユーザーが希望に近いものを選ぶという状況だと思いますので、ユーザー側で契約によって解決しろと言っても実際は相当難しいのではないか、と思っています。

そういう意味では、サービス提供者側に、コンサルタントのような機能が期待される部分もあるかもしれません。実際にコンピューターのシステム開発なんかについては、どういうシステムをつくるかという点に関するコンサルタントのような業務と、実際のシステム開発のような業務があるということが言われる場合があるわけですから、クラウドについても同様だと思います。

また、サービス提供における寡占の問題も、クラウドに関しては気になっています。というのは、クラウドサービスのニーズとしてコスト削減があるわけなんですが、コストについてはサービス提供者側からはスケールメリットが大きく影響してくると思うのです。そうすると、多数の顧客を抱え、大量のリソースを持っているクラウド事業者ほど、安価でサービスを提供できるということになり、結果として寡占化が進むことが起こり得るのではないかなということです。そうすると、ユーザーとしては、契約の条件が気に入らないとしても、他の条件を提供する事業者がいない、選択肢がないということになってしまうことになりますから、責任の範囲は契約で明確化すべきと言っても、その実効性がどこまであるのか、という疑問があるわけです。

実際に、携帯電話でそのような状況が生じています。私はまだいわゆるフィーチャーフォンを使っていてスマートフォンユーザーではないのですが、今度買い換えようとしても、もう、店では、フィーチャーフォンなんかは売っておらず、選択肢としてないのですよね。このように、ユーザー側に選択の余地がなくなってしまうということは起こりうる話だと思います。

また、実際のサービスの内容についてどういう保証を求めるかというようなところも問題になってきます。

インターネットベースのサービスでは、従来、ベストエフォートベースのものが主流でした。つまり、インターネットベースのサービスは、その結果を保証しないということがよくあったわけですが、クラウドサービスが事業のインフラ化しようとすると、ユーザーとしては、サービス内容がベストエフォートで何らの保証がないというのでは困るということになり、サービスをどのように保証してもらえるのかという話にならざるを得ないわけです。ユーザーとしては常に100%保証してくださいとお願いしたいところですが、事業者としてはそれは保証しづらい。多分両者が折り合ったところとして、サービスレベルアグリーメントなどが締結されることになろうかと思います。

経済産業省がＳａａＳ向けのＳＬＡガイドラインというのを出していますが、これが結構細かい内容のものになっています。この中には、例えばＳＬＡの一般的な構成要素が記載されています。その構成要素として、例えば、システム上の前提条件や、合意された委託内容がカバーする範囲などがあります。委託範囲については、既に述べた１のサービス内容の明確化とも絡む話ですけれども、何をお願いしているのかを明確にしていなければ、そのサービスレベルも規定できないということになります。

また、各当事者の役割と責任も必要です。ユーザーとＳａａＳ提供者の間で、どちらが何を分担するのかということを明確にしておかないと、お互いに何をすべきかが分からず、何が債務不履行責任になるのかがわからない、という話になります。

また、サービスレベル項目というのがありますが、これが、まさにそのサービス別に設定される評価項目及び要求水準です。例えばそのダウンタイムが何パーセントなどというのがここに入ってきます。また、規定されたサービスレベルが達成されなかった場合にどうすべきかというのが結果対応という形で入ってきます。

この経済産業省のサービスレベルのガイドラインに必要項目のチェックリストがついていますが、このチェックリストも相当に細かいものになっています。これは、どんなことを検討すべきかという点で参考になりますが、やや専門的過ぎて、ちょっとユーザーとしては、使い勝手がよくないかもしれないです。このチェックリストを理解するためにそれなりの知識が必要となるような感じになっています。

ユーザーの側とサービス提供事業者の側では、知識に差があると思うのですが、ユーザーがサービス事業者を適切に評価するには、自分が相当程度の知識を有している必要があるのですね。

なので、そのような知識がないから専門家の提供するサービスを利用したいのに、適切なサービス事業者を選定するためにそのための知識を身につけなければいけないというような感じになってしまっているのですが、この部分をどう解決できるかが、サービス提供者として今後検討していただきたいところかもしれないと思います。

（２）ボーダレス化に関する問題

次に、ボーダーレスの問題に入ります。ユーザーから見れば、クラウドを利用するときに、そのデータがどこにあるかは、本当は、余り関心がないところかもしれません。ユーザーとしては必要なときに使えればいいわけですから。

例えば、ユーザーが知らないうちに、事業者とユーザーとデータの所在国がそれぞれ別々になっているということも十分あり得るわけです。もともとユーザーと事業者の所在国が別々なだけでも問題が生じるのですが、さらにデータの所在国が異なってくるという話になると、ますます面倒くさい話になります。それが影響するものとして、紛争になった場合に、どこの裁判所で紛争が解決できるかという国際裁判管轄の問題があります。

国際裁判管轄の問題は、訴えを受けた裁判所がある国の訴訟法に基づいて、その国に国際裁判管轄があるかないかということを決めることになるので、実際には日本の法律だけを前提にしてみても仕方がないのですが、まず、日本の場合を前提として進めます。

今まで日本の民事訴訟法には国際裁判管轄に関する明文の規定はありませんでした。この点に関しては、最高裁判例等で、民事訴訟法の土地管轄の規定をてこに、民事訴訟法で言う土地管轄が日本にあれば、原則として日本に国際裁判管轄が認められるという考え方がされていました。国際裁判管轄については、本来、他国間で国際的なルールがある方が望ましいので、ハーグ国際私法会議で国際的な統一ルールを決めるための話し合いをしていたのですけども、結局うまくいかず、結局、事業者間でお互いに合意した場合には、その合意したところが裁判管轄になる、という、あってもなくても意味がないような条約になってしまい、しかも、その国際裁判管轄ハーグ条約に加盟している国もあまりいないので、実際上ハーグ条約は国際裁判管轄のためのルールとしてはほとんど有効に機能しない形になってしまいました。日本は国際裁判管轄に関する条約の成立を待っていたのですが、それがうまく行かなかったものですから、国際裁判管轄については、日本独自で民事訴訟法の中で決めてしまおうということになりまして、その結果、2012年４月１日に施行となった民事訴訟法の改正になりました。

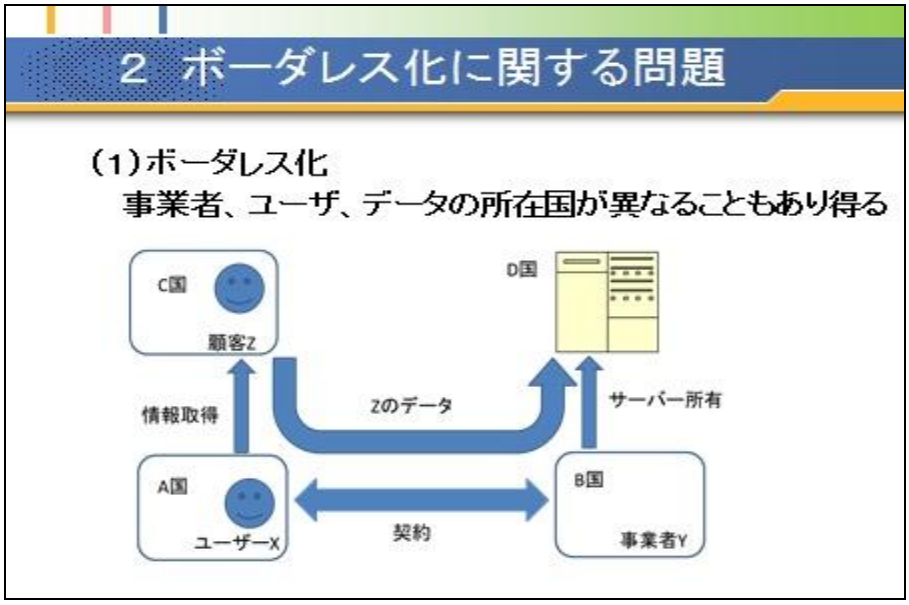
改正された民事訴訟法には、国際裁判管轄に関する規定が入っていまして、従来の最高裁判例などで作られた基準が明文化されています。

原則的な考え方は、従来の土地管轄に関する考え方と同様ですが、注意が必要なのは消費者契約及び労働関係に関する契約の特例です。消費者契約の場合には基本的に消費者の住所が日本にある場合には日本の裁判所に国際裁判管轄があるとされていて、他の国の裁判所を管轄とする旨の合意があってもだめだということになっています。つまり、消費者の住所を考慮してその便宜を考えるべきというのが消費者に関する原則的な考え方となります。したがって、クラウドサービスであっても、サービスを事業者でなくて消費者を相手に提供する場合に、この規定に注意する必要があります。たとえば外国の消費者がユーザーであった場合、クラウドサービスのサービス規約に日本の裁判所が管轄を有すると書いてあったとしても、事業者からユ

ーザーに対して日本の裁判所で訴えを起こした場合、日本の裁判所は管轄を認めてくれない可能性があるということになるわけです。

紛争における責任追及の仕方として、基本的には、契約に基づく債務不履行責任の追及方法と不法行為責任の追及方法があります。下記の例を前提としますと、ユーザーＸと事業者Ｙが契約をしていますから、ＸＹ間での紛争については、契約に基づく債務不履行責任を追及するのが原則形です。

＜スライド15＞



普通の場合は、特にＸが事業者であれば、契約中に国際裁判管轄条項があるので、この点についての合意が優先されます。したがって、契約相手が消費者でない限りは、契約内の合意にしたがって、国際裁判管轄が決まります。国際裁判管轄に関する合意がなかった場合は、その民事訴訟法の規定にしたがって決定されます。

合意がない場合については以下のとおりとなります。この事案でＢ国が日本の場合、つまり事業者が日本所在の場合、日本国外のユーザーであるＸが日本の事業者Yに対して日本で訴訟を提起する場合は、当然、国際裁判管轄は肯定されます。というのは、原告が、わざわざ被告の所在地で訴訟を起こすというものを否定する理由はないわけで、基本的には、どの国でも、被告の所在地での国際裁判管轄は認められています。日本の民事訴訟法でも被告の所在地が日本にある場合、日本の裁判所の国際裁判管轄が認められるということが規定されています。

問題はＡ国が日本の場合です。ユーザーが日本所在で、事業者が日本以外の国に所在している場合ですね。日本のユーザーとしては日本で訴訟を提起したいと思ったとしても、日本は被告の所在地ではありませんので、民事訴訟法が規定するその他の規定に該当するかどうか、と

いうことになります。被告所在地以外で、日本の裁判所に国際裁判管轄が認められる例としては、契約上の債務の履行地が法律上、または合意により日本国内にあるときのほか、財産上の訴えで請求の目的が日本国内にあるか、差し押さえることができる被告の財産が日本国内にあるときがあります。このような規定に該当すれば、日本にいるユーザーは外国のサービス事業者を日本で訴えることができることになります。

また、不法行為に基づく責任追及ということもあり得ます。スライド15の図で、例えばユーザーＸの顧客ＺがＣ国にいて、ユーザーＸは顧客Ｚのデータの保管をクラウドサービス事業者Ｙに委託しており、ＹのサーバーがＤ国にあった場合で、Ｚの情報が漏えいしたことを理由として、Ｚ自身がＹに直接責任追及をするような場合があり得ますが、この場合、ＺとＹの間に契約はないですから責任追及の方法としては不法行為によることになります。

不法行為による責任追及の場合であっても、Ｂ国が日本である場合、つまり、サービス事業者Ｙが日本に所在しており、Ｚが日本で訴えを提起する場合であれば、被告所在地として国際裁判管轄が肯定されます。

不法行為の場合は、事前に国際裁判管轄に関する合意が存在するということは考えられないので、原則としては合意以外の原因で国際裁判管轄が認められるかどうかが問題となるわけです。先ほどのとおり、被告所在地で裁判を提起するのであればほぼ問題なく国際裁判管轄は認められるのですが、Ｚとしては、やはり自分の国であるＣ国で裁判を起こしたいというニーズがあるでしょう。この場合は、Ｃ国の法律で国際裁判管轄の有無が判断されることになりますので、Ｃ国が日本であるとして、日本法についての帰結を検討することとします。つまり、顧客Ｚが日本に所在しており、自らの所在地であるＣ国つまり日本で訴えを提起した場合です。民事訴訟法は、不法行為に関する訴えについては、不法行為があった地が日本国内にあるときは日本の裁判所に国際裁判管轄を認めるという規定になっています。ところで、「不法行為地」が何を指すかですが、不法行為地は、不法行為の行われた地のみならず、その損害発生地を含むと考えられています。したがって、サービス事業者ＹがＢ国に所在した場合、その漏えい行為自体ーその不法行為に当たる行為がＢ国で行われたとしても、その結果としての損害がＣ国で生じていれば、Ｃ国が不法行為地に当たるということになります。ただし、不法行為地に関する国際裁判管轄の規定には例外がありまして、「外国で行われた加害行為の結果が日本国内で発生した場合において、日本国内におけるその結果の発生が通常予見することのできないものであったときを除く」という除外規定が存在しています。

したがって、日本国外であるＢ国に所在するクラウド事業者Ｙとしては、たとえば、Ｃ国つ

まり日本で顧客データの漏出に関する損害が発生するとは予想できなかった、という場合は、その旨を日本の裁判所における国際裁判管轄を否定するための理由として主張できることになります。

除外規定がどんな場合に該当するのか、ということは今後さらに裁判結果の積み重ね等で等で具体化されていくのだろうと思いますが、実は、準拠法に関しても似たような規定がありまして、そこでは、例えば、日本の人は使えませんということが明記されている場合や、実際上日本では使えないような場合は、日本で侵害の結果が発生するとは予想できなかったと言えるのではないかという議論がされています。

以上は、裁判がどこの国でできるかという話ですが、裁判がどこの国で行われるかという話と実際の責任の内容がどこの国の法律で決められるかという話は理論上別になります。後者は、準拠法の問題であり、日本の場合は「法の適用に関する通則法」という規定が準拠法に関して規定しています。これも割と最近（とは言ってももう６年くらい経ちましたけど）改正された法律で、この前は「法例」という片仮名まじりの大変古い法律だったのですが、これが全面改正されて、「法の適用に関する通則法」になりました。

日本の裁判所に国際裁判管轄が認められれば、日本の裁判所が審理を行うことになりますが、その場合、次にどこの国の法律に基づいて実体的な権利義務を判断するのか、ということが問題になります。「法の適用に関する通則法」は、この部分を規定する法律ですので、日本の裁判所での審理は認められるが、実際の権利義務は中国法やシンガポール国法によって判断されるというのはあり得る話です。

責任追及の方法として契約責任に基づくものと不法行為責任に基づくものがあるのは、先ほどお話ししたとおりですが、契約に基づく場合は、通常は、準拠法に関する条項が存在するであろうという点は、国際裁判管轄の場合と同様です。そして、準拠法に関する合意があれば、やはり、その点に関する合意が優先することも同じです。万が一準拠法に関する条項がなかった場合に、「法の適用に関する通則法」は、「最も密接な関連がある地の法による」と規定しています。同法は「最も密接な関連がある地の法」についても規定していて、原則として、不動産に関する取引を除いては「特徴的な給付」を行う当事者の常居所地法となります。

上記を前提とすると、クラウドサービスの場合は、ユーザーは基本的にはお金を払うだけですので、これを特徴的な給付とは言わないでしょう。サービスそのものが当該契約に特徴的な給付ということになろうかと思いますので、準拠法に関する合意がなければ、原則として、サービス提供事業者のある国の法律が適用になることになります。

ただし、準拠法の場合も、国際裁判管轄の場合と同様、消費者契約の特例がありまして、消費者契約の場合は、消費者が主張する場合は、消費者の常居所地の強行規定が適用されるとされています。この場合、契約で準拠法に関する合意があっても、合意がない場合で特徴的給付を行う当事者の常居所地が消費者のそれと異なっており、原則としてはそちらの国の法律が適用される場合であったとしても、消費者が自分の常居所地の強行法規を援用した場合にはそれが適用されることになります。したがってユーザーXが日本国外の例えば香港に常居所地を有している消費者である場合は、Xが香港の消費者保護法の適用を要求した場合には、日本の裁判所は香港の消費者保護法を適用することになります。つまり、契約で準拠法を記載していても意味がなくなる可能性があるので、それが消費者を相手にする場合には気をつけておかないといけないリスクです。

不法行為に関して、国際裁判管轄に関する民事訴訟法の規定と少々異なるのは、民事訴訟法では「不法行為地」という語を使っていたところ、「法の適用に関する通則法」では加害行為の結果が発生した地の法によるという言い方をしておりまして、こちらでは、結果発生地であることを明確にしている点です。

ただ、ネットがからむ場合の結果発生地がどこなのか、というのは非常に難しい問題になってしまうのですが、一般的には、ここでは物が壊れるなどの物理的な状況を想定されていまして、物が壊れたという場合には、その壊れた場所の国の法律であることが明確です。オンラインのサービスの場合は、加害行為の結果発生している場所はどこなのかということ自体が相当難しい問題なので、この規定によってもそれほど明らかとは言えない部分もありますが。なお、先ほど国際裁判管轄でちょっとお話ししたとおり、この不法行為に関する準拠法の規定には例外がありまして、「ただし、その地における結果の発生が通常予見することのできないものであったときは、加害行為が行われた地の法による」という旨規定されています。

ところで、今までの説明で分かるとおり、国際裁判管轄でも準拠法でもサーバーの所在地のD国って検討の過程で出てこないんですね。なので、実際に耳にする話として、法律に関する問題の検討においてサーバーの所在地は関係ないという意見をよく聞きます。事業者の所在地が問題なのであって、サーバーの所在地は問題ないという議論がされることがあり、確かに、今ご説明したとおり、それは一面では真実だとは思うのですが、全く関係ないということはないのではないか、と個人的には思います。例えば、判決の執行まで考えたら、サーバーの所在地が問題となり得る場合もあると思うのですね。

事業者、あるいはユーザーが任意に判決に従ってくれれば問題はないと思うのですが、判決

の名宛人が判決内容を任意に履行してくれないときには、強制的に判決内容を実現させなくてはならないことになります。この場合の判決の執行の作用というのは国の権力ですから、日本の判決の結果を例えば中国で執行しようと思うと、日本の裁判所の効力ではできなくて、中国の裁判所なり何なりの助力を得ないと実現できないわけです。この場合、実はサーバーの所在地を、考えておく必要が出てくる場合があると思います。

過去の裁判例を見ますと、ファイルローグ事件という著作権侵害の判決がありまして、ピア・ツー・ピアのサービスを提供していた日本の事業者に対する判決なのですが、この事件は、事業者は日本に所在していたのですけどもサーバーはカナダにあったんですね。１審判決では、サーバーがカナダにあるということを全く考慮せず、日本の裁判所において日本法を適用して判決しています。控訴審では、適用法が問題とされていますが、東京高裁は、当該サービスによるファイルの送受信のほとんど大部分が日本国内で認められていることと、当該サービスに関する稼働・停止等が被告である事業者が決定できることなどから、著作権侵害行為が実質的に日本国内で行われ、被侵害権利が日本の著作権法に基づくものであるとして、条理（差止請求の関係）ないし法例１１条１項（不法行為の関係）により日本法が適用されると判断しています。このように、判断に際しては、サーバーの所在地は問題になりませんし、また、事業者が判決を任意に履行すれば問題にならないと思います。また、差止命令なども、執行方法が間接強制の場合、日本の裁判所が日本の事業者に対して処分しますので、やはりサーバーの所在地は問題とならないでしょうが、判決の内容によっては、それを実現する場合に、直接の強制や代替執行などの方法による場合もあり得るので、そのような場合にはサーバーの所在地が問題となる場合もあるのではないかと思います。

先に述べたとおり、ここでの説明は、日本で裁判が起こされた場合に、日本の裁判所がどう判断するかということに関するものです。別の国で裁判が起こされた場合に、別の国の裁判所がどう判断するかというのは、その国の訴訟法なり、その国の準拠法に関する法律なりで判断されることになりますので、実際には、該当する国の法律を検討する必要があります。実際にクラウドサービスを各国で展開しようとする場合には、該当国の法律を調査することになるのだろうと思います。

今まで説明したのは、基本的には損害賠償や差し止め等の私法上の権利に関する問題に関してですが、公法に関する問題も検討する必要があります。こちらのほうがむしろ問題な部分もあります。というのは、公法の法執行というのは、国家権力の作用ですから、原則、他の国では行使できません。属地主義が原則であり、日本の公法は日本国内にのみ適用されるというこ

とになります。

公法の典型的なものが刑法ですが、刑罰を課するというのはまさに国家の主権の作用であり、刑法については、日本国内において罪を犯したすべての者に適用されることが原則です。ただし、「国内において罪を犯した」ということの意味が、昔の裁判例で、その構成要件となる行為の一部が日本国内で行われた場合のみならず、構成要件的結果が日本国内で発生した場合も含む、とされています。

先ほどの不法行為の行為と結果の話に似ていますが、殺人を例にあげますと、人を刺したという行為が例えばアメリカ国内で行われて、刺された被害者がすぐには亡くならず、日本まで来て、日本で亡くなってしまったという場合は、日本国内で死亡という結果が発生しているので、日本国の刑法が適用されるという結論になるのですね、ただ、この裁判例は大正時代のものですから、ネット上で発生するような犯罪を当然のことながら想定していません。

そうすると、今のように国境を越えてインターネットが普及している状況で、結果が日本で起こっていれば、いつでも日本の刑法が適用になるのかは、なかなか難しい問題です。例えばオンラインの賭博を例に考えてみます。日本では賭博は刑法で処罰される行為ですが、オンライン賭博としてアメリカのサーバーから日本のユーザー向けに賭博に関するサービスが提供されている場合、提供者側の行為は日本国内では行われていませんが、賭博という結果が日本国内に生じていると言えるわけです。では、アメリカのサービス提供事業者を日本の刑法で処罰できるのかと考えると、難しい問題ということになろうかと思います。

特に、日本では違法だが、アメリカでは適法な行為の場合、それを日本の法律で違法だから、ネット上で提供するなと言えるかどうかについても難しいということが言えると思います。このようなことを考えると、大正時代の裁判例を前提として、国内で罪を犯したというのが、結果が生じた場合も含むという考えた方がネットを介した行為にもそのまま適用になるのかちょっと分からないところです。また、仮に日本の刑法が適用されるとしても、例えば警察による捜査や逮捕などは、まさに国家権力の作用ですから、日本の警察がアメリカ国内で捜索・差押えを行うことはできません。とすると、このような場合に、日本の刑法が適用されるとしても、どの程度実効性があるかということがまた別の問題として残っているということになります。

これらの実効性などを考慮して、実際上は日本国外の人には公法が適用されないと考えられがちです。

ネットに関しては、その辺が実際に問題になっています。日本で継続的に事業を行う場合は、日本に代表者を置いて登記をしなければならないということが会社法に規定されているのです

が、事実上日本での登記がないまま、アメリカや他の国からオンライン上でのみ、日本向けのサービスを提供している事業者があります。ところが、そのような事業者に対しては、何も取り締まれない結果となっているところが問題になっています。

個人情報保護法などは、行政法規なので公法ですね。個人情報保護法は、事業者が行うべき公法上の義務が規定されていて、違反行為に対しては、行政からの指導・監督等がされることになっています。個人情報保護法が日本国外の事業者に対して適用されるのかがよく問題にされています。外国の事業者が日本所在の個人から個人情報を取得する場合に、日本の個人情報保護法が適用になるのかという点は、いまだにはっきりされていない。日本の個人の個人情報を守るという点からすれば、取得するのが日本の事業者であろうと外国の事業者であろうと本来同じはずなのですけども、その公法的な性質から適用されるとは言いにくいのだと思います。

この点に関して、ＥＵは、個人情報をＥＵ外に移転させてはいけないという形でわりときちっと規制していますが、日本の個人情報保護法は、国外への移転についても何も規定を置いていませんので、いつまで経っても、適用関係がふにゃふにゃしたまま、だんだん問題が大きくなりつつある状況だと思います。

クラウドサービスとの関係では、例えば、個人情報の第三者提供などの点が問題になります。個人情報保護法では、第三者に個人情報を提供する場合には、原則本人の同意が必要とされていますが、クラウドサービス事業者にデータを預けるときに、いちいち本人からの同意が必要だとすると大変煩雑なことになります。一般にはクラウド事業者は個人データの取扱いの委託を受けたものとして、第三者には当たらないと解釈されると言われていますが、この点についての疑問も呈されています。

また、既に述べたとおり、個人情報の海外移転については、特段の規制がなく、個人情報の保管場所については、個人情報保護法では規定されていません。したがって、クラウドサービスを利用した場合、データが国外に保管されていたとしても、それがただちに個人情報保護法上問題とならないようにも見えます。

なお、ガイドライン等では、個人情報の国外での保管についての記載があるものもあります。例えば平成21年７月総務省から出た「ＡＳＰ・ＳａａＳ事業者が医療情報を取り扱う際の安全管理に関するガイドライン」がその一例です。これは、ガイドラインですので、これに拘束力があるのかという問題はありますけれども、同ガイドラインでは、「所管官庁に対して法令に基づく資料を円滑に提出できるようＡＳＰ・ＳａａＳサービスの提供に用いるアプリケーション、プラットホーム、サーバ・ストレージ等は国内法の適用が及ぶ場所に設置すること」とい

う記載があります。この場合には、妥当する情報を国外で保管すると、安全管理義務違反に問われる可能性があると思われます。

また、民間のガイドラインですが、平成22年４月付けの次世代電子商取引推進協議会による「民間部門の電子商取引に係る個人情報保護に関するガイドライン（Ver7.2）」にもデータの海外移転に関する記載があります。同ガイドラインには、データを海外移転する場合にはあらかじめ公表の上、本人の明示的な同意をとる必要がある旨の記載があります。とはいえ、ネットビジネスにおいてオンラインで日本向けに多数の海外事業者が日本のユーザーから情報を取得し、本人からの同意を得ずに、どんどん本国にこれらのデータを送っているときに、日本の事業者だけ個人情報の海外移転に本人の同意が必要とされるというのも、日本の個人についての利益状況は同じであるだけに、なんだかバランスが悪い。どっちも同じような規制が適用にならないとおかしいじゃないか、競争として公平じゃないじゃないか、と思います。

なお、海外移転そのものについては個人情報保護法では規定がないのですが、海外でデータが保管されることの帰結として、データの所在地が分からない場合には、分からないということ自体が問題になる可能性があります。

というのは、クラウドサービスのユーザーが個人情報取扱事業者であり、取扱にかかる個人情報のデータをクラウドサービス提供者に預けている場合、個人情報取扱事業者には安全管理措置を講ずる義務や、委託先の監督を行う義務が課せられています。にもかかわらず、どこにデータがあるのか分からないという状態にいるとすると、本当にこれらの安全管理措置に関する義務や監督義務を講じていると言えるのかについて疑問が生じるのです。

この点に関しては、少なくとも、どこの国にデータが措かれているかぐらいは契約で規定しておきましょうというようなことが言われています。ただ、契約でそのような内容を規定できるかどうかについては、サービス利用契約に関する部分で説明したとおり、利用者とサービス提供事業者のバーゲニングパワー等の問題や、寡占化による選択肢の減少などが影響してくる可能性があります。

公法については、当事者間の合意では決めることができませんので、当該サービスに適用される各国の公法公法的な規制は、きちんと検討しておく必要があります。

（３）セキュリティの問題

あとはセキュリティ一般のお話ですけれども、セキュリティについてなぜあえてここで説明するかというと、ユーザーの懸念点としてこの点が一番強く意識されているからです。総務省

で、クラウドサービスを利用しない理由についてのアンケートをとったところ、「セキュリティに不安がある」という選択が37.9%ということで一番多かったという結果が発表されています。その他は、クラウドサービスの導入に伴う既存システムの改修コストが大きいというものもありますが、これは、もともとクラウドサービスをコストダウンのために利用したいというニーズからみれば、導入によってコストが増加しては意味がないということになるので、ある意味わかりやすい、合理的な理由なのですね。ところが、一番多数であったセキュリティに不安があるという点については、セキュリティとして何が不安なのかが不明確なままの、ある意味漠とした不安とも言えるのではないかと思われます。

したがって、ユーザーの不安の原因が何かを分析しないと、サービスが発展しない可能性があるので、クラウドサービスにおけるセキュリティについて、検討した方がいいのではないかと思っています。

ユーザー側と事業者側の双方の話を聞いてみると、このセキュリティに関する意識が、両者で一番すれ違っているのではないかと思われる部分があります。例えばユーザー側としては、クラウドサービスを利用すればするほど、自分の手元にあるデータや機能等が少なくなります。アプリケーションもクラウド上で利用することを選択すれば、データのプロセス作業も自分ではできないということになりますから、クラウドサービス事業者がいきなりサービスを中止などした場合には非常に困るなどという不安感を持っているわけです。

ところが、サービス提供事業者との話をすると、ここで感じているユーザーの不安は、クラウドを利用していない場合と事実上同じではないか、というような感覚を持っているようなのです。つまり、データ等を自分の手元で保管したり、処理していたりしたとしても、通常、そのようなシステムまわりの面倒を見ているのは少人数のことが多いから、担当者が突然辞めてしまったら事実上システムがストップしてしまうのと同じではないか、というようなことをおっしゃるのです。確かに、そういう面は否定できないと思うのですが、そうは言っても、ユーザーとしては、問題が生じるのが、自分の支配領域内か自分の支配のできない領域外かという点は、大きな差として意識されているところだと思うので、そこが事実上同じだと言ってみても、ユーザーの側ではなかなか納得ができないのではないかと思います。

そうすると、サービス提供者としては、何らかの解決策を提示する必要があろうかと思うのですが、解決策を提示するためには、セキュリティが問題とされる理由を分析していくしかないわけです。そうすると、例えばクラウドサービスの利用には、インターネット接続が必ず付随するので、そういう通信インフラの影響を必ず受けてしまう点が問題である、とか、あるい

は、クラウドサービスでは同一システムを複数のユーザーが利用していますから、他のユーザーが行う行為の影響を自分が受けることを問題としている、または、システムやリソースの構築がクラウド事業者側で行われており、ユーザー側からは見えずで把握しづらい点が問題だ、というような分析がされてくるのではないかと思います。

最終的な解決方法としては、契約によることになるのではないかと思うのですが、ユーザーとしては、何が重要かを把握できないことがあります。サービス提供事業者がサービスをストップした場合に、どういう状況が確保されれば、自分は困らないのかという点は、システムの内容が細かくわかっていなければ想定できません。それを全部ユーザーの側で把握しろといってもなかなか難しい。その点に関する解決方法としては、第三者の認証を使うことなども１つの方法だと思います。自分で判断することが難しい場合に、判断能力を信頼できるだれかのお墨つきがあるかないかによって、決めようというものです。

その一例が一定の規格を満たしているかを参考にするというものですが、ＩＳＯとかＧＳＭなどのセキュリティの規格は必ずしもクラウドに対応しているとは言えません。というのは、これらの規格は、利用者自身が所有している情報資産を自分で管理するというところを前提としているので、クラウドのように、人のリソースで人の情報資産を運用するような状況に、そのまま適用できるとは言いかねる部分があります。

クラウドに特化した規格の必要性というところで、経済産業省が「クラウドサービス利用のための情報セキュリティマネジメントガイドライン」というのを出していて、これに基づいてクラウドに対応したＩＳＯの規格を作ろうとしているといわれています。

この経済産業省のガイドラインの目的は、事業者によって行われているシステム運用がユーザーから見えるようにすることで、サービス利用のための安心感を増進しようとするもので、そのための方策をまとめたものがこのガイドラインになります。

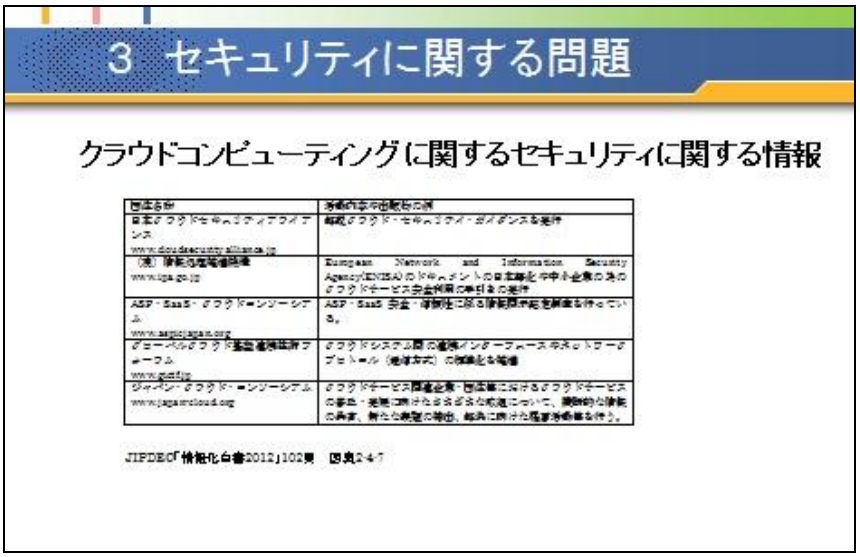
相当細かいものになっておりますが、このガイドラインについている附属書Ａ、Ｂ、付録がクラウドサービス利用に係るリスクの一覧やクラウドサービス利用におけるリスクアセスメントの実施例などを記載しているもので、参考になります。ただ、これも相当細かいので、ユーザーとしては、これを理解すること自体が一苦労かもしれません。

そこで、ユーザー視点でもう少し簡単にできないかという観点からのものとして、特定非営利活動法人のＡＳＰ・ＳａａＳ・クラウドコンソーシアムの「クラウドサービス利用者の保護とコンプライアンス確保のためのガイド」や独立行政法人情報処理機構が平成23年４月に出した「中小企業のためのクラウドサービス安全利用の手引き」があります。これらは先ほどの経

済産業省のガイドラインに比べると、分かりやすいものになっていると思います。ユーザーとしては、まずは、このあたりのものを参考にするのが実際的かもしれません。

クラウドのセキュリティに関する情報は、下記の団体等から提供されていますので、これらをチェックしていると、今行われている動きなどが分かると思います。

＜スライド28＞



あと、セキュリティの問題の最後に、ＯＳＳの利用というのを一応検討しておかなくてはいけないかなと思っております。ＯＳＳとは、オープンソースソフトウェアの略であり、アンドロイドなどもそうですけれども、コストなどの観点から、最近、よく利用されるようになっています。

ＯＳＳについては、注意点もありまして、ＧＰＬをちょっと見た人ならわかるとおり、ＯＳＳはそれ自体に保証がないという問題もさることながら、ソースコードを開示しろという要求が極めて厳しいものがあります。特にＧＰＬ系のライセンスは、ソースコードの開示が要求される範囲がきわめて広範にわたります。ソースコードの改変が要求される場合でも、よくあるのは、改変した場所のみのソースコードを開示せよ、というものなのですが、ＧＰＬの場合は、ＯＳＳとリンクでつなげた場合でも全体についてソースコードの開示の対象となります。しかもＧＰＬのライセンスを策定しているＦＳＦ、フリーソフトウェアファウンデーションという組織がアグレッシブなところがあり、自分たちの自由を守る（つまりソフトウェアの著作権を権利者に行使させない）ために、自分たちが賛同者の著作権を行使する、というような運動を展開していて、ＧＰＬの違反に関する情報をネットで集めており、違反に対して著作権者として訴訟を起こすということもしていますので、ＧＰＬについては十分注意が必要となります。

クラウドにおいては、ソースコードの開示も極めて重要な問題です。自分のプロプリエタリーなソフトウェア、自分の財産として費用と時間をかけてつくり上げてきたソフトウェアについて、そのソースコードを開示しなくはいけないということになると、資産開発のための費用と時間がパーになってしまいます。クラウド上での運用方法によっては、上記のような結果になる場合があり得ます。

通常のＧＰＬはオンラインサービスでそのまま使うだけだったらソースコードの開示は要求されていませんが、ＧＰＬの変則形にＡｆｆｅｒｏというライセンスがあります。そのＡｆｆｅｒｏは、オンラインで使っている場合、つまりサーバー上で走らせているだけでもソースコードを開示することが要求されます。

また、リンクでつなげたら全部がソースコードの開示対象となるというように、ＧＰＬのソフトウェアは実装方法が問題になります。実際にクラウドサービスの事業者には、サービス規約の中で、自らが権利を有しているプログラムのソースコードが開示されることのないように配慮した条項を入れているところもあります。規約の条項に入れるだけで、どこまで実効性があるかという問題はありますけれども、サービス提供事業者側として取りうるのはそれくらいしかないかもしれませんので、そのような規定を入れておいて、利用者から質問を受けたときに、説明をして注意を喚起するというようなことは意識してもいいのではないかと思います。

特に、最近はスマートフォンのアプリなどで個人のプログラム開発者がふえている関係で、スマートフォンのプログラムについて調査したところ、６割だか８割だかが違反だったという調査結果があったという話も聞きましたので、事業者として自衛できることはしておいた方がいいのかもしれません。

ただ、本日、ＩＴメディアか何かの記事で、ＯＳＳの傾向が反転してきて減少傾向であるというものをみましたので、そのような傾向が続けば、この点は今後はそれほど気にする必要がなくなるかもしれません。アンドロイドもバージョンいくつかからから有料にするというような話があるようですし、そうだとすると、ＯＳＳだからコストが安いという話にはならない可能性はあるかもしれません。

【５．付録】

あとは、付録としてスマートフォンの話をちょっとだけします。スマートフォンは、今すご

い勢いで普及していて、先ほども申し上げたとおりフィーチャーフォンが欲しくても、もうフィーチャーフォンは販売されていないような状況です。１年ぐらい前に私がフィーチャーフォンを買ったときでも、既にスマートフォンの方がフィーチャーフォンより２万円ほど安いような状態でしたから、よほどのへそ曲がりじゃない限りスマートフォンを買うだろうと思われるので、現状はある意味当然の状況だと思います。

スマートフォンの特性として、常にネットワークに接続していることから、クラウドとの親和性が高いと言われています。実際にスマートフォン導入企業の57％でクラウドを利用しているということですから、クラウドとスマートフォンの相互利用というのが今後フォーカスされていくのかなと思います。

また、スマートフォン特有の問題として、携帯電話と同じで常に持ち歩くために、個人との結びつきが高いということがあげられます。スマートフォンにおける個人情報が今すごく問題になっておりまして、スマートフォンのアプリが勝手に個人情報を外に発信しているというニュースが何度か報道されているのはご案内のとおりだと思います。

スマートフォン利用のリスクは、スマートフォンはその機能として携帯というよりむしろＰＣに近いのですが、利用者の意識がそれに対応していないというところにあります。利用者は、通常の携帯電話からの買いかえで利用を始めるものですから、携帯電話と同じ感覚で使ってしまうのです。特に青少年の有害情報の関係では、青少年のスマートフォン利用というのは非常に問題なっています。

クラウドサービスと親和性が高い点がどのように影響するかというと、スマートフォンそのものには大したデータが入っていなくても、スマートフォンを通じてクラウド側に大量に蓄積されたデータが流出するという可能性があげられます。

スマートフォンを落とした場合、データ流出に関して特段の対策がされていないとすると、クラウド側のデータをスマートフォンを通じて全部持っていかれてしまうということになりかねないわけです。そういうリスクという形で影響してきます。

あとは個人との結びつきの高さが個人情報やライフログの蓄積に関して問題になります。また、ブリング・ユア・オウン・デバイスという利用形態、つまり、もともとプライベート用だったスマートフォンを業務上も利用させることが進んでいることについての問題も生じており、これらを今後どのようにしていくかという検討が進められています。

スマートフォンのセキュリティの話は相当ホットトピックなので、あちこちで検討されています。たとえば、日本スマートフォンセキュリティフォーラムがガイドラインを発表してます

し、総務省のスマートフォンクラウドセキュリティ研究会でも検討が行われています。

また、総務省の「利用者視点を踏まえたＩＣＴサービスに係る諸問題に関する研究会」が過去にライフログ活用サービスに関する検討を行っていましたが、その延長線上の問題として、スマートフォンを経由した利用者情報に関する検討をしています。まさにアプリの個人情報に関する問題です。

メールソフトを使うときに自分のアドレスブックを利用するのは当たり前だと思うんですけれども、アドレスブックを利用するということの意味が、単にソフトの機能上それを利用するということなのか、アドレスブックの情報を外部に提供しているのかが、パーミッションなどを見ても分からない、という問題や、音楽ソフトなのに位置情報をとっているなど、ソフトの機能上、不要な情報をとっていることなどがあるという問題について、検討しています。この辺のところはそのうち報告書が出るので、興味のある方は見ておかれるといいかなというふうに思います。

ちょっと海外の検討状況なんかも足しておきましたけれども、極めて駆け足になってしまいましたが、ちょうど１時間半ということなので、終わりにさせていただこうかなと思います。

○司会　ありがとうございました。

何かご質問等ございましたら、この機会にお聞きになっていただけます。

【質疑応答】

Ｑ　スライド24の「クラウドサービスでセキュリティが問題とされる理由」のところで、最終的に契約で解決する案というのが出ているんですが、具体的には。

上沼　契約で、結局そのサービスレベルなり何なりとかで責任を明確化するしかないという、一番最初にお話ししたようなところになるかと思います。

―　実際にセキュリティに対する不安を持っている利用者に対して、契約でというのはちょっとよくわからないのだが。

上沼　例えば、そのデータの所在地がわからないみたいなところも含めて、セキュリティの不安として言っているわけですけれども、そこについては、例えばそのデータの所在地を限定するという契約を入れるとか、あるいはインターネットの接続が不安だという場合であれば、そのサービスレベルアグリーメントでダウンタイムがいくらか、という形で入れるとか、そういう個別の規定を入れていくしかことで解決していくしかないのではないかな、という趣旨です。

○司会　ほかにございますか。

それでは、きょうはどうもありがとうございました。

以上