第９回
ＯＤＲ推進検討会
議事録

第１　日　時　　令和３年５月２１日（金）　　自　午前１０時０２分
　　至　午後　０時００分

第２　場　所　　法務省赤れんが棟３階「第五教室」

第３　議　題　　１．開会
　　２．湯淺墾道教授による御講演及び質疑応答
　　３．ＡＤＲ法関連の規律の見直しにつき今後検討を予定している
　　論点について
　　４．閉会

第４　議　事　（次のとおり）

議　　事

○渡邊参事官　それでは，定刻となりましたので，第９回ＯＤＲ推進検討会を開会させていただきます。

今回も多くの方にウェブ会議により会議に参加していただき，ありがとうございました。この会議での発言方法につきましては，これまでと同様に挙手機能等を活用していただければと思います。

それでは，垣内座長，よろしくお願いいたします。

○垣内座長　おはようございます。私の声は聞こえていますでしょうか。

はい，ありがとうございます。

本日もお忙しい中，検討会に御参加いただきましてありがとうございます。

それでは，早速ですけれども，本日の議事に入りたいと思います。

まず，事務局から資料の説明をお願いいたします。

○渡邊参事官　本日の資料は，資料１から資料３までの３点となります。

資料１は事務局作成の資料となります。当検討会の検討事項でありますＡＤＲ法関連の規律の見直しにつき，今後検討すべき論点を事務局で整理させていただいたものでございます。詳細は追って説明させていただきたいと思います。

資料２は，本日御講演予定の湯淺墾道先生提出資料となります。湯淺先生には，この後，資料２に基づいてＡＤＲのオンライン化とセキュリティーの演目で御講演していただく予定としております。

資料３は，斉藤委員提出資料となります。湯淺先生の御講演の後に，斉藤委員から御紹介いただく予定としております。

現時点での資料の説明は以上となります。

○垣内座長　ありがとうございます。

資料の方はよろしいでしょうか。

それでは，続きまして，早速ですけれども，本日は，明治大学大学院教授である湯淺墾道先生にお越しいただいております。湯淺先生，どうもありがとうございます。

湯淺先生からは，情報セキュリティーの関係で御講演を頂けるということで伺っております。

それでは，湯淺先生，御発表お願いいたします。

○湯淺教授　垣内先生，御紹介ありがとうございました。

ただいま御紹介を頂きました，明治大学の湯淺でございます。本日はこのような機会を頂きましてありがとうございます。

本日は，ＡＤＲのオンライン化に当たりまして，一般的にどのようなサイバーセキュリティー上の懸念点があるかということを御紹介させていただき，サイバーセキュリティーの現状ということを，少し御紹介をさせていただく予定でございます。

その後，ただいまこちらの会議でも御検討を進められていると伺っておりますが，セキュリティーの観点から，こういう点に検討していただく必要があるのではないかということを，二，三御紹介をさせていただきまして，最後に，ＡＤＲに参加をされるのは一般の国民の皆様かと思いますが，特に参加者が留意すべき点ということを，御紹介をする予定でございま

す。

大体３０分ぐらいお時間を頂戴いたしまして，私の方からお話をさせていただく予定でございます。

それでは，資料を共有させていただくことにいたします。

サイバーセキュリティーの現状ということでございますけれども，サイバー犯罪，特に不正アクセスですね，他人のコンピューター等に不正に侵入をする行為，それから，コンピューターウイルスを作る，あるいはそれを他人のコンピューターで実行するというような行為につきましては，１０年ぐらい前から全く減っていない，年々増え続けているというような現状でございます。

最近のサイバー犯罪でございますけれども，インフラのように非常に広範に影響を与えるようなものへの大規模な攻撃ももちろんあるわけですが，目に見えない資産を狙ったものが増えているという状況がございます。すなわち，企業の顧客であったり，特許情報であったり，ノウハウであったり，財務情報や人事情報，戦略や新製品・サービス，あるいはＡＤＲで正に扱われているような紛争に関する情報ですね，そういうような目に見えない資産を，不正アクセスやコンピューターウイルス，マルウエアに感染をさせて窃取しようとする，そういう攻撃が非常に多い，また，それによる被害が増えているということでございます。

日本の場合，サイバー犯罪被害の報告義務とかはございませんので，全体としてどれぐらいの被害が出ているのかということを，客観的に把握するのがなかなか困難でございますけれども，個人情報漏えいについては，現行の個人情報保護法では，漏えいしたときの通知義務というのはございませんが，個人情報保護委員会のガイドライン上，それを本人に通知をすることが望ましい，二次被害を防ぐために公表することが望ましいとされているところから，漏えいが起きてしまいましたということが公表される場合がございます。そういう新聞報道，あるいは企業のウェブサイトなどで公表されるものを，毎年日本ネットワークセキュリティ協会というところが収集をして公表しておりますけれども，大体年間５００万件から七，八百万件の漏えい人数で，１件当たりの漏えい人数が６，０００人，７，０００人，８，０００人程度，そして，公表されている限りで，年間このような事案が８００件程度起きておりますので，恐らく実数はもっともっと多いのだと想像されます。これは，公表していないという事例もあると思いますし，漏えいしていることにそもそも気が付かないという企業や団体等が多いということかと思います。

このような個人情報の漏えいの原因でございますけれども，これはもう，この数年大きな変化というのはございませんで，これも日本ネットワークセキュリティ協会の調査結果でございますけれども，大体は紛失をしてしまったとか，置き忘れをしたというケースでございます。それから，２番目に多いのは，例年誤操作でございまして，誤操作の多くは，ＢＣＣでメールを送ろうと思ったら，うっかりＣＣで送ってしまったというようなケースでございます。それから，管理ミスで，公開すべきでないところを公開するような設定にしてしまった，クラウドの操作ミス等が多いということでございます。その後，不正アクセスに遭った，それから盗難，それから内部から情報を持ち出されたという内部犯罪，それとコンピューターウイルスに感染したというようなものが４分の１でございますので，大体全体の４分の３は何らかの実はヒューマンエラーであるということです。残りの４分の１が外部から，あるいは内部犯行も含めた要因によって起きているということでございます。

したがいまして，ＡＤＲのセキュリティーということをお考えいただく際には，実は，操作ミスが非常に多いのだということですね。もちろん，外部からの攻撃という要因もあるんですが，セキュリティーに関するトラブル，インシデントの多くは，実は内部のヒューマンエラーであるということを，御留意を頂ければと思います。

また，最近の事例でありますと，どこからそういう情報が漏れてしまうのかということにつきましては，不正侵入された，それからコンピューターウイルス，マルウエアに感染させられたという経緯が多いということでございます。

最近のコンピューターウイルス，マルウエアは二分化をされておりまして，ランサムウエア，身代金型というように呼ばれるものがあり，これに感染すると，ファイルだとかフォルダーが開かなくなってしまいます。開かなくなってしまって，それで，身代金を送金すると，開くためのパスワードが送られてくるので，それでやっと開けるようになるという型のものです。それから，もう一つの型は，このマルウエア，コンピューターウイルスに感染しても，特に何も起きないというものです。何も起きないんですが，知らない間に外部から侵入をされてしまって，中のデータを全部抜き取られてしまうという型のコンピューターウイルス，マルウエアですね。コンピューターウイルス，マルウエアに感染する被害は，そのように二分されている状況にあるということでございます。

もう一つ，このヒューマンエラーの一種と申し上げていいのかもしれませんが，設定権者，あるいは利用権者のパスワード設定や管理が甘いということも原因でございます。同じパスワードを使い回したり，初期設定のまま使っている，あるいは，誰でも類推できるような簡単なパスワードを設定してしまうので，それによって他人に乗っ取られてしまうというケースが増えております。

また，コンピューターだけではなくて，ネットワークにつながっている複合機でありますとか，インターネットにつながっている監視カメラ，あるいは，最近ではスマホやタブレットの被害というのも増えているという状況でございます。

その他，本当に多種多様なサイバー攻撃がありまして，正に技術進化とともにこのサイバー攻撃も非常に増えているし，サイバー攻撃もどんどんどんどん進化をするというような状況にございます。したがって，なかなか対策も難しいわけでございまして，特に，今この資料の９ページ目に書いておりますゼロデイ攻撃，ソフトウエアにセキュリティー上の脆弱性が発見されたときに，その問題が公表される前に，その脆弱性を突いて攻撃するというものについては，まだウイルス対策ソフトなどが対策をアップデートする前に攻撃されてしまいますので，これをやられると，なかなか対策も難しいと言われております。

その他，多種多様なサイバー攻撃があるということを，１０スライド目では御紹介をさせていただいております。

特に電子メールを使った攻撃では，標的型電子メール，それからＡｄｖａｎｃｅｄ　Ｐｅｒｓｉｓｔｅｎｔ　Ｔｈｒｅａｄ，ＡＰＴと呼ばれるものが非常に問題とされております。どういうことかと申しますと，これは，特定の方を相手として偽メールを送るわけですね。偽のメールを送って，至急ここにアクセスしてくださいと誘導する場合もございますし，資料を御参照くださいと回答するというような場合もございます。例えばですが，今日，私も法務省の方から今日の資料を頂いたわけでございますけれども，法務省の方からきちんと送付されてきているのでいいわけですが，法務省をかたって，偽の人間がこの資料と称するも

のを送る。開いてみたら，そこにはコンピューターウイルスが仕込まれていて，感染してしまったというようなケースが非常に多いわけですね。

したがって，今回，今日御参加の垣内先生も御参加されております，法制審議会のＩＴ化の部会で，私が電子メールでやり取りをする方法に過度に依存することは，あまりよくないということを申し上げました。電子メールでのやり取りというのは，今申し上げましたような偽メールにお互いに被害に遭う危険性やコンピューターウィルスに感染する危険性が非常に高いということでございます。裁判所からのメールと言われれば，普通国民は慌てて開いてしまいますし，逆に当事者の方からメールで送られてくれば，裁判所の方もうっかり開いてしまうと。そうすると，お互いに開いてしまって，ここでコンピューターウイルスに感染ということが起こり得ます。もちろん，それを防ぐ技術として幾つかあるということも，法制審議会では御紹介をさせていただきましたが，場合によっては，そういう保護技術を採るということも必要なのかなと思っております。

それでは，また資料共有の方に戻りますが，もう一つ，恐らくこのＡＤＲを御利用されるのは，大企業，大きな組織の方もおられると思いますが，必ずしも大きな組織だけではなくて，中小の事業者，あるいは個人の方が利用されるというケースも少なくないと思います。あるいは，ＡＤＲ事業を実施される事業者，それ自体も，必ずしも規模が大きいとは限らないのではないかなと考えておりますが，そういう中小の事業者というのは，特にサイバー攻撃を受けやすいと言われております。その理由は，セキュリティー対策がやはり大きな組織に比べると不十分である，それから専門家がいない，委託先に任せっぱなしになっているとか，組織にシステム担当者がいないとか，いても１人ぐらいしかいないので，ほかの人はよく分からない，そういうことから，サイバー攻撃を受けたのに気付かない。あるいは，１台のパソコンで，あっちにアクセスしたり，こっちにアクセスしたり，多目的に使っているので，非常に攻撃に遭いやすくなるというような事情ですね。あるいは，これもよく聞く言葉なんですが，「うちには大したものはありませんよ」と，「うちに攻撃してくる人なんかいませんよ」ということを，よくおっしゃるわけですが，自分のお持ちの資産の価値に気付いていない，こういう理由から，中小の事業者がサイバー攻撃を受けやすいと言われているわけでございます。

さて，以上が前段の話でございまして，サイバーセキュリティー問題の現状ということについてお話をさせていただきましたので，この後の時間をお借りいたしまして，オンライン化に当たってどのような点を御考慮いただく必要があるのかということを，お話をさせていただきます。

一般に，セキュリティーの対策を考えるときには，１９９２年のＯＥＣＤの情報セキュリティーガイドラインで示されましたＣＩＡ，Ｃｏｎｆｉｄｅｎｔｉａｌｉｔｙ，機密性，それからＩｎｔｅｇｒｉｔｙ，完全性，それからＡｖａｉｌａｂｉｌｉｔｙ，可用性の３点を確保するということが重要と言われております。このうちのＯＥＣＤのガイドラインのＣＩＡを更に，それに準拠しつつ日本語化したものとしまして，日本産業規格，旧日本工業規格のＪＩＳがございまして，ＪＩＳＱ２７００２という規格では，情報の機密性，完全性及び可用性を維持することに加え，真正性，責任追跡性，否認防止性及び信頼性のような特性を維持することを含めてもよいというように述べられております。今日はＡＤＲについてのお話でございますが，民事訴訟，訴訟ということになりますと，まさに証拠の真正性，あるい

は否認防止，信頼性というような要件も要求されてくるかなと思います。

このうち，機密性は，これは情報へのアクセスを認められた者だけがその情報にアクセスできる状態にすること，Ｉｎｔｅｇｒｉｔｙ，完全性は，情報及び処理方法が正確かつ完全であることの保護，情報の不正な改ざんがないこと，情報の処理結果の誤りがないこと，情報に欠損がないこと，Ａｖａｉｌａｂｉｌｉｔｙ，可用性につきましては，情報へのアクセスを認められた者が，必要時に中断することなく，情報及び関連資産にアクセスできる状態を確保することということでございます。この三つ，このＣとＩとＡの三つを両立させるということが，情報セキュリティー対策であるということになります。

さて，このような前提を踏まえまして，このＡＤＲ手続の電子化をどのように考えていただくかということでございますけれども，一番最初に検討していただく必要があるのは，やはり法令が何を要求しているかの明確化ということでございます。この法令の要求を明確化した後，その法令の要求を遵守しつつ，電子的に代替するには，どのような技術的手段を採ればよいかということの検討が必要になります。

それから，関係者の確定で，先ほどのＣＩＡで申しますとＣの部分になりますが，手続に関わる関係者を確定するとともに，誰にどの情報へのアクセス権限を与えるかということを設定する必要がございます。

それから，これは特にＯＤＲ事業を実際に提供する事業者の方の側の方に当てはまるかと思いますけれども，それにどういうリスクがあるか，どういう脅威があるか，またどういうところでサイバー攻撃を受けたりしやすいか，また内部要因，人的要因はどういうところに危険性があるかということを分析していただく必要がございます。例えば，先ほどの例で言えば，メールでやり取りするということにしていたら，偽メールが送られてきて，うっかり開いてしまう。あるいは，関係者にまとめてメールを送る方が手っ取り早いので，まとめて電子メールで送ることにして，ＢＣＣで送ることにしたら，ＣＣで送ってしまったとか，そういう様々な要因がございます。

それから，業務委託先，端的に言えば，様々なクラウドサービスやメッセージサービスを利用する場合には，先方の事情で障害が発生して使えないということがあり得ます。その使えないときにはどうするかというリスクの想定が必要でございます。

様々なそういうリスクや脅威があるとしまして，情報通信の世界では，リスクをゼロにすることはできないと言われておりますので，そういうリスクや脅威にどのように対応するかを事前に策定をしておく必要がございます。端的に言えば，ＡＤＲで正に今，問題になっている事案の情報をうっかり漏らしてしまった，あるいは漏れてしまった，その漏れてしまった，漏らしてしまったらどうするか，万が一漏らしてしまったとき，漏れてしまったときの被害を最小化するにはどうするかということを，様々な技術だとか様々なサービスなどを組み合わせて考えていくということでございます。

実際被害が起きてしまったらどうする。コンピューターウイルスにやられて，手元のファイルが全部やられてしまった，あるいは流出してしまったときに，どうすれば一番被害を最小化できるかということの被害発生時の対応をあらかじめ決めておくということが必要ということでございます。

その際に検討すべき点でございますけれども，セキュリティー対策というのは，一般的にきつく，固くやればやるほど，逆に利便性は落ちてしまいます。したがいまして，その利便

性と秘密保持の必要性とを比較考慮しながら，適切な水準を設定するということが必要でございます。その際には，従来の対面手続では，一体どの程度の利便性や秘密保持性が要求されていたのかということを確認していただき，それと比較をしながら，適切なセキュリティー水準を設定していただく必要がございます。

それから，オンライン化に当たりましては，当然この個人情報保護，個人情報の漏えい等が起きないようにすることや，プライバシーの保護という必要性も出てまいります。一番恐らく問題になるのが，本人確認とアクセス制限をどうするかというところだと思います。これは，オンラインでの手続全般に要求される問題でありますが，これにつきましても，今申し上げましたように，従来の手続との比較が必要ということでございます。

さらに，様々な民間事業者が提供しているツールを利用する場合には，約款の契約を精査していただき，法律の専門家の皆様の前で，釈迦に説法でございますけれども，要するに，約款上，こちら側がどういう権利があるのか，あるいは先方は，サービス提供事業者側はどういう免責になっているのかということを十二分に確認していただくこと，特にバックアップはどちらの責任になっているのかということを，よく確認していただく必要がございます。

それから，特にクラウド等を利用する場合には，サービスレベルアグリーメント，ＳＬＡと言っておりますけれども，何％の確率で利用できないことがありますよということが，あらかじめ明示をされておりますので，何％の確率で使えないことがあるよということを検討していただく必要がございます。

それから，ＡＤＲでも全くあり得ないとは言えないのは，そういうサービスを提供する事業者自身が当事者になってしまったということです。この場合はどうするかということも検討していただく必要がありますし，また，特定の事業者の提供するサービスだけに依存し過ぎると，その事業者から変えられなくなると，俗にベンダロックと言っておりますけれども，そういうことがあり得るということの留意も必要になるわけでございます。

一例としまして，本人確認手続をどうするかということを，セキュリティーの観点から考慮すると，こういうことになります。従来の手続，対面手続では，そもそも何を，何によって，どうやって確認をしていたのか，その際に，対面ではどの程度の厳格性が求められていたのかということを，まず確認をしていただく。それをオンライン化する際に，対面確認で行っていた何を，何によって，どうやってということを，オンラインに置き換えることができるか，できないか。できないとすれば，それは何か新しいものに置き換える必要があります。その新しいものに置き換えるとすれば，どんな要素を使うことができるかということを検討する必要がございます。

それから，もう一つ必要なのは，本人確認は，対面の方がオンラインよりも厳格で行うべきなのか，対面による確認の厳格性とオンラインによる厳格性は同じでよいのか，それとも，オンラインの方がなりすましの危険性が強まるので，対面時よりも厳格にする必要かあるのかということでございます。これも結構重要な点で，例えば，今日のようにオンラインのツールを用いているときに，カメラをオンにする，オンにしない，これは，もちろんカメラをオンにしたからといって，直ちになりすましの危険性が増す，減るということにも限りませんが，しかし，相手が事前にある程度顔などを知っている人物であれば，カメラに映る姿を確認することによって，ある程度本人性が確認できるということになってきますので，そういう検討をしていただく必要があるのかなと思います。

それから，これはむしろＯＤＲ事業者というよりも，ＯＤＲにオンラインで参加する個人の方々の留意点でありますが，パソコンやスマホ，タブレット等を紛失する，あるいはなくすということに留意をしていただくこと，それから，常にＯＳなどは最新版にアップデートをしていただくこと。やはり個人の方であれば，このＯＤＲ用にわざわざ１台専用の端末を用意するということは考えにくいので，いろんなアプリなどを入れてしまうと思いますけれども，その出どころに注意して，怪しいものを入れない。今日のように遠隔ミーティングツールを使用する際には，チャットに出るＵＲＬをクリックしたら，そこでマルウエアに感染したということもあるので，チャットの利用に注意をしていただくこと。また，先ほどのプライバシー保護という点で申しますと，背景に，例えば，窓の外等が映り込んでいますと，そこから住所が特定されてしまう危険性もあるので，背景に注意をしていただくということ。

何よりも，パスワードの管理ですね。ここは，非常に難しいのは，そういう点で言いますと，以前は，定期的にパスワードを変更してもらうことがセキュリティーの向上になると言われていたわけですが，最近は，定期的にパスワードを変えてもらうと，やはり人間は覚え切れませんので，ついつい同じパスワードを設定してしまいます。むしろ同じパスワードを設定する方が危険と言われるようになってきておりまして，定期的なパスワード更新というのは，必ずしも求めない傾向になっています。パスワードを使い回すと何が起きるかといいますと，資料はフェイスブックの例ですが，いろんなサービスを乗っ取られてしまうということですね。乗っ取られて，こういう感じで詐欺のメッセージが送られたりするような危険性がございます。

最後に，民間サービスを使うときに，どんな点に留意すればよいかということですが，例えば，チャットツール等につきまして，先ほど約款上の地位の問題点ということを申し上げました。この約款上の地位の問題点につきましては，先般，いわゆるＬＩＮＥ問題が起こったのを受けまして，政府からガイドラインが出されておりまして，その中で，事業者と，それからそれを利用する側との地位の問題につきまして，非常に整理がなされておりますので，公的な業務，公共性を有する業務における利用時には，非常に参考になる内容になっております。

また，このような記載がございます。要機密情報を含む業務連絡等でメッセージアプリを利用する場合，ＩＳＭＡＰに基づき・・・とありますが，ＩＳＭＡＰとは何かと申しますと，政府情報システムのためのセキュリティー評価制度でございまして，要するに，政府が求めるセキュリティー要件を満たしているクラウドサービスを，あらかじめ評価，登録しておく制度でございます。政府が公共サービスのために政府の求めるセキュリティー要件を満たしているサービスは，これですよということの評価が行われておりますので，それを利用すれば比較的に安心だということになります。

大変駆け足で恐縮でございましたが，大体３０分程度お時間を頂きましたので，私からの発表は，以上でございます。

どうも御清聴ありがとうございました。

○垣内座長　湯淺先生，どうもありがとうございました。大変参考になる貴重な情報を多数頂けたように思います。

そうしましたら，委員あるいはオブザーバーの方々から御質問等ございましたら，是非，せっかくの機会ですのでお願いできればと思います。いかがでしょうか。

佐成委員，お願いします。

○佐成委員　佐成です。どうも，貴重な御講演ありがとうございました。

いろいろお聞きしたいんですけれども，一つだけちょっと教えていただきたいのは，クラウドサービス固有といいますか，先ほどお話がありましたＳＬＡですか，何％使えなくなることがありますよというような，そういった御説明がございましたけれども，クラウド固有のセキュリティー問題というのは何かあるのでしょうか。その辺りだけお聞きしたいと思います。

○湯淺教授　御質問ありがとうございました。

クラウド固有のセキュリティー問題は，いろいろ指摘されておりますけれども，まず，非常に大きな点で言えば，そのクラウドサービスのサーバーが国外に置かれているのか，国内に置かれているのかということでございまして，国外にサーバーがありますと，日本国の法律の効力が及びませんし，また逆に，相手国の法律の規定で，そのサーバーの中に置いてあるデータの中身が，相手国政府に見られてしまうというような危険性も生じるということが指摘をされております。

この点に関しましては，ＬＩＮＥ問題でも問題になったのはそこでございまして，中国の業務委託先のスタッフがアクセスをしていたこと，あるいは韓国の国内にデータが置かれていたということが，問題になったということでございます。

それから，仮に国内にサーバーが置かれていたとしてもということでありますが，やはり今も御質問にあったとおり，クラウドサービスが障害を起こすということがあり得ます。何％の可能性でやはり障害が起きてしまって，サービスが提供できなくなりますよということがあらかじめ示されていますので，その間はサービスを利用できなくなります。例えばですが，今，非常に普及しているマイクロソフト製品等でも，これが一時的に障害を起こしますと，全くログインできなくなるので，メールも使えなくなってしまうとか，クラウド上のデータにも全然アクセスできなくなるというような，要するに，全く何もできなくなってしまうということが，ある確率で起こり得るということですね。したがって，それが起きちゃったときにはどうするかということを，あらかじめ想定をしておく必要があるということでございます。

それから，これはクラウドサービスだけの問題ではございませんが，やはり外部サービスを利用する際には，常にバックアップということを念頭に置く必要がございます。クラウドの方が安心だ，安全だと言われるようになってきておりますし，幸いなことに，現在のところでは，大きな事業者のデータが完全に失われてしまったという事案はございませんが，しかし，過去にデータセンターのデータが障害で全部消えてしまったとか，そういうことは多々起きておりますので，やはりクラウドサービスを利用する場合にも，クラウド上に全部データを置いてあるから安心ということではなくて，バックアップを適切に取っていただくことが，非常に重要と考えております。

駆け足ですが，クラウドサービスの問題点というのは以上でございます。

○垣内座長　どうもありがとうございます。

佐成委員，よろしいでしょうか。

○佐成委員　はい，結構でございます。

○垣内座長　ありがとうございます。

それでは，ほかの委員の方，いかがでしょうか。

上田委員，お願いします。

○上田委員　上田でございます。ありがとうございます。

本日は大変貴重な御教示を頂きまして，ありがとうございます。

最後の方のＩＳＭＡＰについて若干お伺いしたいんですけれども，クラウドサービスに関する政府のセキュリティー要求水準を，ＡＤＲやＯＤＲの世界に引き付けて考えますと，例えば，今後，民間事業者がＯＤＲサービスのためのウェブシステムなどを開発して，それをクラウドサーバー上に乗せて運用し,それを，さらに，個々にＡＤＲ機関が民間事業者と利用契約を結んで利用するという形態も考えられると思うのですけれども，このＩＳＭＡＰの基準というのは，クラウドサーバーの，例えば，ＡＷＳであるとか，グーグルのクラウド，プラットフォームなどの方に及んでいて，個々のＯＤＲのために構築されたシステムの方には及ばないという理解になるのでしょうか。御教示いただければと思います。よろしくお願いします。

○湯淺教授　上田先生，どうも御質問ありがとうございました。

現時点では，ＩＳＭＡＰという制度の趣旨は，御理解のとおりでございます。したがって，対比して考えますと，今，例えば，地方自治体のサービスの一つに，マイナンバーカードをコンビニに持っていくと，住民票等がコンビニで取れるというような住民票のコンビニサービスがあると思いますけれども，あれは，地方共同法人でありますＪ―ＬＩＳが，事実上，マイナンバーを使ってやり取りをする自治体間のネットワークを言わば管理をしているわけですが，そのＪ―ＬＩＳにおきまして，マイナンバーを使う情報ネットワークに接続できるＡＰＩの基準を示しまして，このＡＰＩはＪ－ＬＩＳが審査した結果，つなげてよいということにしましたという，そのＡＰＩの認証制度というのを持っています。

したがって，コンビニのマイナンバーカードを使った住民票の提供サービスなどは，Ｊ―ＬＩＳが認証したＡＰＩを使って実現しているサービスということになりますが，現時点では，ＩＳＭＡＰというのは，そういうような個々のＡＰＩに相当するようなものを認証するというものではないということで，それは，上田先生の御理解のとおりかと思います。

○垣内座長　ありがとうございます。

上田委員，よろしいでしょうか。

○上田委員　はい，ありがとうございます。

○垣内座長　それでは，ほかの皆様，いかがでしょうか。

出井委員，お願いします。

○出井委員　出井です。湯淺先生，どうもありがとうございます。

私からは，プリミティブな質問をさせていただきたいと思います。

ＯＤＲというか，ＡＤＲをこうやってオンラインでやる場合のリスクとして，よく言われていたのが，今日はＴｅａｍｓでやっていますけれども，ビデオカンファレンスシステムを使う場合に，メールのやり取りがテキスト情報として外部からアクセスされる危険というのがあるというのは，一般には分かるんですけれども，こういうＺｏｏｍ会議での情報，映像であるとか，あるいはバーバルなコミュニケーション，これが外部からアクセスされるというリスクは，やはりあるのでしょうか。そのリスクは，メールでのやり取りのリスクに比べて，何か有意な差があるのでしょうか。これが第１の質問です。

それから，もう一つ，先生のお話の中で，最初の方に裁判のＩＴ化との関係で，メールに過度に頼り過ぎることが危険であるというお話がございました。その場合に，それに対するプロテクションというのもいろいろあるということでしたが，逆にメールに頼らない，それ以外のコミュニケーションツールを使うべきであるというサジェスチョン，方向性もあるのでしょうか。その場合には，それは，どういうオルタナティブなのか，この２点，お聞きしたいと思います。

○湯淺教授　どうも御質問ありがとうございました。

まず，１点目の方でございますけれども，今日，ほとんどのテレビ会議，オンライン会議システムは，内容は暗号化をされた上でインターネット上やり取りをしておりますので，この内容が，直接的に中身が窃取されてしまうということは，技術的には考えにくいと思います。ただ，Ｚｏｏｍについては，この一部のデータが中国国内のサーバーにあるということが明らかになっておりますので，そういう意味で，一部の組織ではＺｏｏｍは使わないということにして，ＴｅａｍｓやＷｅｂｅｘを使うようにしているということもあるかと思います。これは，どちらかというと，国際政治的な要因ということになるのかなと思います。

メールに比べて安心なのかということでありますが，結局のところ，今申し上げましたように，今日，こうやってやり取りしている内容が直接傍受されたりして，その中身が漏れる危険性は技術的には低い。しかしこうやってアクセスをさせていただいているわけですが，このアクセスをする権限それ自体が外に漏れていたりすると，ほかの人間が入ってきてしまうという危険性があるわけですね。先般，何かＩＯＣの遠隔会議ツールを使った記者会見か何かでも，最後の方にオリンピック開催反対というのを訴えた人が乱入してきたとかいう報道がございましたが，あれは恐らく，会議に参加するためのパスワードなどが何らかの，人為的に漏れたのか，それとも漏らされたのか分かりませんが，恐らく漏れていたんだと思いますね。それで参加されてしまったんだということだと思います。

そういう意味で申しますと，メールに比べて，こういう遠隔会議ツールを使った方法はどうなのだということについて言いますと，ＩＤやパスワード，参加の権限等をきちんと管理している限りにおいては，メールよりも危険ということはないということになります。

２番目の御質問と少し関連してきますけれども，当然この，今日，ファイル共有で先ほど私のプレゼン資料を映しましたが，例えば，チャット機能などを使ってその場でファイルをやり取りしたりすることも，オンライン会議のツールによっては可能ですね。当然このチャット機能を使ってファイルをやり取りするという際に，それをうっかり開いたら，そのファイルの中にコンピューターウイルスが仕込まれていて，それで感染しちゃったというリスクは，これは，電子メールの添付ファイルをやり取りしているのと同じリスクであるということになります。

２点目の御質問なんですけれども，私が電子メールのやり取りに頼り過ぎるのは危険と法制審議会で申し上げたのは，三つほど理由がありまして，一つは，ＡＤＲではあんまり考えにくいのかもしれませんが，民事訴訟では，海外に原告や被告の方がいらっしゃって，海外から参加をするということも想定されますが，具体的に申しますと，例えば，Ｇメールなんかは，中国から一般的な環境では使えないんですね。そうしますと，メールだから必ず世界各国どこへでも届くというわけではないという意味で，余り頼り過ぎると危険ということを申し上げたのが１点目。

それから２点目は，ＡＤＲではそこまで考えにくいのかもしれませんが，物すごく膨大な書類のやり取りがされて，それを，添付ファイルをメールにたくさん送り付けてきて，それをお互いにやり取りしていると，メールに付いている添付ファイルを整理したり何なりするだけでも，すごい人手が必要になって，かえって電子化をすると効率の妨げになりかねない危険性があるということ，もちろん電子メールの添付ファイル自動仕分システムみたいなものを入れれば，また話は別ですが，そういう危険性がありますね。さらに，添付ファイルというのは非常に危険です。添付ファイルを開く際に，そこにマルウエアが含まれていないかどうかを事前に検知をして，マルウエアが含まれていたら開かないというような，もちろんそういうセキュリティーソフトもありますし，そういうツールもありますが，添付ファイルというのはつい開いちゃうわけですよね。そうすると，メールの添付ファイル経由でコンピューターウイルスに感染するというケースが非常に多いので，メールの危険というよりも，むしろ添付ファイルの危険という点で申し上げたということでございます。

３点目が，なりすまし偽メールの問題で，要するに，送信者のメールアドレスを偽装すれば，いかにも法務省を装ってメールを送ることも可能ですし，いかにも裁判所のように装って偽メールを送ることも可能です。もちろんこれも対策技術はちゃんとあるんですが，そういう意味で，なりすましの危険性があるということを申し上げました。そういう理由で，電子メールへの過剰な依存は危険ということを申し上げました。

代替のやり方として何がありますかということですが，添付ファイルに変えては，ファイルを一遍クラウド上などのストレージに上げて，それをダウンロードするためのリンクをメールで送るというような仕組みも，最近は普及してきております。あるいは，多要素認証も普及してきました。最初，サービスのアカウントを作るときには，ＩＤとパスワードだけではなくて，携帯電話の番号も入力してもらって，携帯電話のショートメッセージにも何か番号を送り，事前に送ったＩＤ，パスワードとこのショートメッセージに送られてきたものと，両方入れないと，最初アカウントを開設できないようにする仕組みとか，そういうような対策技術がいろいろございます。

ちょっと御説明が長くなりましたが，以上でございます。

○出井委員　ありがとうございました。

ストレージサービスは，国際仲裁の場面では既にかなり使われていますけれども，私はあまり理解していなくて，単に分量が多いから，こういうのを使っているのかなと思っていたのですが，今のお話だと，セキュリティーの面でも，ストレージサービスというのは意味があるというお話ですね。どうもありがとうございました。

○垣内座長　ありがとうございます。

ほかにいかがでしょうか。

山田委員，お願いします。

○山田委員　山田と申します。

湯淺先生，大変分かりやすい御説明をありがとうございました。

２点お伺いできればと思います。

一つは，資料の１６ページの手続の電子化の考え方の一番下で御指摘の，被害発生時の対応というところです。リスクゼロにはできないということで，事後の対応が重要となることからＯＤＲ事業者にこの対応手続を明確化しておく必要があるだろうと思うのですけれども，

これに関して，何かプロトコルのようなものがありましたら，御紹介を頂けましたら大変有り難く存じます。

それから，もう一点は，１８ページで本人確認に関してですけれども，最後の問題提起で，オンラインの方がなりすましの確率が高くなるとも言えるので，より一層厳しい確認が必要だという考え方もあり得るとおっしゃられて，それは確かにおっしゃるとおりだなと思うんですけれども，その際に，具体的にどういう形で確認をするのがよろしいか，既に実務等の基準がありましたら，教えていただければと存じます。

よろしくお願いいたします。

○湯淺教授　どうも御質問ありがとうございました。

まず，１点目の御質問につきまして，基本的に，インターネット上では，一度流出してしまったデータというのは，回収するということが非常に難しいのが現状でございます。したがいまして，万一ファイルなどが流出してしまっても，すぐにはその中身を見られないようにするということの方が，予防的には重要ということになります。

ですから，例えばですが，先ほどクラウドサービスやストレージサービスを使ってファイルをやり取りするということを御紹介しましたが，なお，そのやり取りされたファイルに別のパスワードを掛けておくということにすれば，万一ローカルにダウンロードされたファイルが何らかの理由で漏えいや流出してしまったとしても，直ちにその漏えい，流出してしまったファイルを，第三者が開けて見ることはできないということになります。

あるいは，最近不正競争防止法の改正がございまして，限定提供データという考え方が導入されております。これは，ファイルに，今申し上げましたような，例えば，パスワードを掛けておいたりして，第三者が開けないような仕組みにしておく。これが万が一，例えばですが，どこかに流出をしてしまって，別の第三者がそれをもって使おうとしているということが明らかになったような場合に，民事で差止め訴訟を提起できるとかいうような，そういう法制度も少しずつ整備されつつあります。しかし，それも，誰がそれを持っているか分からないことには提訴のしようもありませんし，まずは，その重要な情報については，万一流出しても，すぐには見られないような状態にしておく方が，予防的には役に立つということでございます。

もちろん，今般国会で改正されました，プロバイダー責任制限法の手続を使って，万一その情報が公開されてしまっているのであれば，その削除を求めたりとか，そういうことも，もちろん事後的には可能ではありますが，しかし，一度拡散してしまうと，しらみ潰しに訴訟を起こさないといけないということにもなってしまいますので，なかなか一度流出してしまった情報を全部削除するのは難しいということです。

それから，２点目の本人確認なんですが，これ，特に統一的なプロトコルというものは，現状ではございません。まずは，それぞれの各サービスなり各オンライン手続の性質に応じて，どの程度厳格な本人確認をしていただくかということになります。

恐らく，現時点で最も厳格な本人確認を取っていると思われるのは銀行や金融機関のサービスで，原則的には，その場でオンラインでアカウントを開設するということはできない，１回郵便等で必要な文書を送って，本人確認がなされた上で，アカウント等が開設できる仕組みになっていて，かつ，アカウントを開設する際，これは，郵便で送る場合もあれば，電子的な手段でコピー等を送るということもあるのでしょうが，マイナンバーカードだとか運

転免許証とかの公的な身分証明書の提出を求めるということで，本人確認も厳格に行っているかなと思います。

あるいは，公的な手続で言えば，いわゆる電子納税がそうでございまして，これは，基本的にはマイナンバーカードを用いるか，あらかじめ国税庁，税務署に身分証明書等を送っておいて，専用のＩＤパスワードを交付してもらうかということで，本人確認がなされた上でないと利用できないというサービスになっております。そういう公的な身分証明書を使った本人確認と，それから郵便物を経由することによる居住地確認を取るのが，最も厳格な本人確認ということになります。

逆に，最近取られることが多いのは，メールアドレスに一定まず招待メールを送って，それを更にクリックして，そのメールが確かな本人に届いているということが確認できた上で，アカウントを開設できるようにすると。あるいは，先ほどもちょっと御紹介申し上げましたが，電子メールだけではなくて，携帯電話の方にもショートメッセージを送って，その両方をクリックしてアクティブにしないとアカウントを開設できないようにするという方法も，最近は増えているかなと思います。

○山田委員　ありがとうございました。

○垣内座長　どうもありがとうございます。

そのほか，さらに御質問等おありでしょうか。

佐成委員，お願いします。

○佐成委員　すみません，１点ちょっと教えていただきたいんですが，今，山田先生が御指摘された部分に関連しての御質問です。要するに，リスクをゼロにすることが非常に難しいということですから，被害発生時に備えて二次的にいろいろ対応策を採っていくということかと思うんですけれども，その中には，保険契約というものは，考えられるのでしょうか。

取り分け，関心があるのは，ランサムウエアの脅威とのバランスについてです。企業幹部の身代金目的誘拐に備えた保険契約は存在していますが,そこでは犯罪者が保険金を目当てにして犯罪を助長する可能性が指摘されていますけれども，ランサムウエアとの関係でも保険という問題が出てくるのかなと思ったんで，その辺りの検討状況というのがもしあれば，教えていただきたいと思います。

○湯淺教授　ありがとうございます。

実はサイバーセキュリティー保険というのは，損保各社から商品化をされております。個人情報流出保険とか，あと，最近，弁護士事務所向けのサイバーセキュリティー保険などの商品もいろいろあると聞いております。

ランサムウエアの点でございますけれども，現状では，日本の保険会社各社のセキュリティー保険では，ランサムウエアの身代金の支払には保険金を出しておりません。これは，御質問のように，犯罪者を利することになるということからかと思います。

これは，実は国際的にも揺れている点でございまして，アメリカのＦＢＩは，従来はランサムウエアの犯人に身代金を払うべきでないと言っていたんですが，払わないことには，その組織のクリティカルな情報が回復できないので，組織全体の維持に差し障るような場合には，払うこともやむなしというようなニュアンスの文書を公表しております。アメリカの場合には，サイバーセキュリティー保険でランサムウエアの身代金は支払うことがあるようでございます。

しかし，現時点では，日本では，それはいわゆる反社会集団を利するということで払っていません。逆に，日本のサイバー保険では，例えば，原因究明費用だとか，あるいはどこからやられたのかということを究明しないと，またやられてしまいますので，そのどこからやられたのかということを経路を明らかにする費用等々，それから，商品，サービスにもよりますが，その他バックアップからデータを元に戻すための費用等々もカバーされる商品もあると聞いております。

○佐成委員　ありがとうございました。

○垣内座長　どうもありがとうございます。

さらに御質問等ございますでしょうか。

挙手はございませんですかね。

もしすぐにないようでしたら，私の方からも少し御質問させていただければと思います。

１点目は大変細かい資料の内容についての理解の確認なんですけれども，本日御提供いただいたパワーポイント資料の７ページ目のところで，漏えいの原因について御紹介を頂いておりまして，左の方で不正アクセス等々，ウイルスを含めて，合わせて４分の１ぐらいと，逆に言うと，残りの４分の３はヒューマンエラーということだという御紹介があったところですけれども，右の円グラフを拝見しますと，ウイルスということで見ますと，上の方でしょうか，ワーム・ウイルス１０件，１．３％と，こういうものがありますけれども，ウイルスとかマルウエアということに限って申しますと，全体の中ではかなり比率としては少ないと見てよろしいのでしょうか。

○湯淺教授　垣内先生，御質問ありがとうございます。

これは，飽くまでも日本ネットワークセキュリティ協会が個人情報漏えいについて公表されている部分，新聞，報道その他で公表されている分の集計ということで，資料を作成されているものです。しかし，先ほど申し上げたように，大体例年傾向は変わらないわけですが，少なくとも公表された分についてはということで，コンピューターウイルス，マルウエアに感染してしまって，そこから情報を漏えいしてしまったという例は，ヒューマンエラーによるものより意外と少ないということでございます。

ただ，実はこれも，先ほどちょっと申し上げましたが，コンピューターウイルスの多くは，今は感染していることをなるべく隠すようなものになっておりますので，分からないんですね。感染して，いつの間にか情報が漏れているというケースが非常に多々ございますので，そういうものは当然，本人も気付いていないわけですから，こういう調査対象にもなってきませんので，実際の被害というのはもっと多いんだろうとは思っております。

○垣内座長　分かりました。どうもありがとうございます。

それから，もう一点なんですけれども，特に内容的には，１９ページの辺りのお話に関係するのかと思いますが，ＡＤＲの場合ですと，ＡＤＲの事業者側できちんとセキュリティー対策を採るということが一方であり，そのときに，この１９ページに書かれていますように，ＯＳ等を最新版にアップデートするですとか，あるいは，直前にお尋ねしましたウイルス等との関係では，ウイルス対策ソフトをしかるべくインストールしておくとか，いろいろあるかと思うんですけれども，ＡＤＲの場合ですと，手続の中で出てくる情報について，ＡＤＲ事業者，手続実施者の側と当事者双方との間で，一定範囲で共有されると，やり取りが行われるということになるかと思います。

そのときに，そこで出てきた秘密性，秘密として保護される必要があるような価値のある情報について，ＡＤＲ事業者はきちんとやっているけれども，当事者の側で，例えば，持っているＰＣがウイルスに感染してしまっているであるとか，ＯＳが古くてすぐに外部から侵入されてしまうであるとかいった可能性というものも，抽象的には存在するのかなと思われるんですけれども，そうしたときに，例えば，ＡＤＲ機関の側で，当事者に対して，どこまでその辺りの配慮を求めるというか，注意をするのかと。

例えば，ちゃんとウイルスソフトは入れていますかとか，ＯＳは最新のものに更新してくださいというようなことを，ＡＤＲ機関の側から当事者に対して注意喚起したり，あるいは促したりとするようなことも，考えられるのだろうと思うんですけれども，その辺り，どこまで対応していくということが，一般の民間の事業，あるいは公的な事業等との関係で，相場観と申しますか，もし現状これぐらいが普通ではないかというようなことがあおりであれば，御教示いただければと思いまして，お尋ねさせていただきました。よろしくお願いします。

○湯淺教授　垣内先生，どうもありがとうございました。

お尋ねの点につきましては，実際にそういうＡＤＲの当事者がマルウエアに感染したりして，当事者から秘密性の高い情報が漏れてしまった，それによって，もう一方の当事者から，例えば，それによって損害が被ったとか，精神的な被害を受けたというような，いわゆる法的な責任の議論が出てくるということを，そういう蓋然性ということを前提とした御質問であったのかなと拝聴しておりましたが，その場合，まず，ＡＤＲ機関側に責任がどの程度あるかということでございます。

過去の個人情報漏えい等の判例等を見ますと，まず，公的機関からの個人情報の漏えい等が起きた場合，職員等に，例えば，私物のＰＣを使ってはならないとか，業務情報を外に持ち出してはならないということを，内部の規則で周知してあったにもかかわらず，それに違反をして職員が外部に例えば持ち出し，それが漏えいしたということまでは，その予見可能性については，そこまでは予見できないということで，その場合には公的機関等が責任を負わないとした判例は存在しております。そのこと自体に批判もございますけれども，判例上はそういう周知をしてあったのであれば，それ以上，それに反してまで漏えいが起きるようなことは予見できなかったという判断がされているところでございます。

一方で，民間事業者がどの程度まで社内，あるいは派遣事業者等々も含めて，注意義務を払っていたと，どの程度までの対策を打ち，どの程度までの技術的な対策を打っていれば，相当な注意を払っていたと言えるのかということにつきまして，これは一連のいわゆるベネッセ訴訟が判示をしているところでございます。

あの事件は，内部犯行であったというやや難しい事情があったわけでございますけれども，少なくとも，現時点において，日々セキュリティー対策も進化していますので，この技術を使っていたから，漏えいが起きても相当程度の注意義務を払っていたことになる，この技術を使っていなかったから，それは予見できたはずなのに，予見可能性があったというように，各技術，この対策とかこの技術とかと，そういうのを個別に射程を当てて，それによって有責性を判断するという一般的な基準を確立するところまでは，判例全体としていっていないのかなと思います。

そういう意味で申しますと，現時点でＡＤＲ事業者が，ＡＤＲの参加者に対してどの程度

の注意喚起をして，どの程度の，逆に例えばですが，システムには古いＯＳのパソコンからはつながせないようにするとか，そういうような，どの程度までやればＡＤＲ機関が万一のそういう情報漏えい時に免責になるのか，参加者の方からの情報漏えいが起きたときに免責になるのかということについては，これをやっておればよい，これをやっていなかったら駄目というような，明確な線がちょっと引きにくい状況にあるのかなと思います。

したがいまして，恐らく一般的に言われているセキュリティー対策というものを周知をし，その実践を求めるというのも，恐らく最低限のラインなんだと思いますけれども，逆に言うと，それをやっていたから免責されるという保証もないという，ちょっと曖昧な状況にあると思います。

これが，個人情報保護法改正で，今度の改正で個人情報取扱事業者に対しては，漏えい時の本人通知義務だとか，監督機関である個人情報保護委員会への報告義務等が入ったときに，さらに事業者，ＡＤＲ事業者への責任というものがどの程度変わっていくことになるのかは，現時点ではまだ予見できないというところはございます。

それから，当事者にどの程度の責任を負わせることができるか，これも，結局，むしろ当事者の地位ですよね，ＡＤＲ機関を利用して，現にＡＤＲに参加されている当事者の方の地位が，一体どういう地位にあるのか。また，先ほどと同じですが，不可抗力と見る，これから先は不可抗力，予見可能性がなかった，逆にこの程度なら予見できたはずというのが，個別の事案においてどのように判断されるかというのが，ちょっとまだ現時点におきましてはお答えしにくい。特にＡＤＲの場合は，弁護士のように，いわゆる士業で，相当の専門職として一般の方よりも更に注意義務を払うべき存在ではない，一般ユーザーの方が参加されている場合に，一般ユーザーの方にどこまでそういう注意義務が求められるのかというのが，まだサイバーセキュリティーの領域においては確定的でないのかなと思っております。

ちょっと長いお答えになってしまいまして，申し訳ございません。

○垣内座長　御丁寧に御解説を頂きまして，どうもありがとうございます。

なかなか，外にもう基準ができていて，それを持ってくれば足りるというわけでもなく，今日の御報告で申しますと，１７ページの一般的な考え方として示されておりますけれども，利便性と秘密保持等を考慮した適切な水準というものを，ＡＤＲの特質に即して考えていなければならないということなのかなと思って拝聴いたしました。どうもありがとうございます。

さらに追加で御質問等，佐成委員，お願いします。

○佐成委員　すみません，何度も。

今のお話を聞いていて，１点だけ御質問いたします。セキュリティーソフトを導入しているか，していないかで，特に責任に大きく影響するのかどうか，その辺りについて，ちょっと教えていただければと思います。

○湯淺教授　ありがとうございました。

セキュリティーソフトを入れていたか，いなかったかということについては，正直に申しまして，今後の争点にはなりにくいと思います。と申しますのも，ある時点まではセキュリティーソフトを入れましょう，セキュリティーソフトは必須ですねという話もあったんですが，ウインドウズをお使いの方は御案内のとおり，現在のウインドウズ１０にはウインドウズディフェンダーという，ＯＳ内蔵のセキュリティー保護機能が付いていまして，これ，結

構強力でございます。そういうことも踏まえますと，現時点において，セキュリティーソフトを入れていたから責任は軽減されます，逆に，入れていなくてディフェンダーのままで使っていたから軽減されませんということにはなりにくいのかなと思っております。一般のユーザーの方に限った話ですが，そのように思っております。

○佐成委員　ありがとうございました。

○垣内座長　どうもありがとうございます。

渡邊委員，お願いします。

○渡邊委員　湯淺先生，本日は貴重なお話をどうもありがとうございました。

今回の会議に先立ちまして，アメリカの州裁判所のＯＤＲの支援をしておりますＮＣＳＣのテクノロジー担当の方に，州裁判所の方でどのような対策をされていますかということをお聞きしてみたのですが，そのお返事としまして，やはり第三者機関を活用したセキュリティーのアセスメントを行うということが一つ，プライバシー影響評価を求めるというのがもう一つで，本人確認に関しましては，先ほどのスライドにもございましたが，基本的には対面でやっているのと同じ内容で，当事者に関してオンラインを利用することによる過度な負担を掛けないようにというような方針でされているというようなことをお聞きしました。私もこの分野に詳しいわけではなく，お話をその方にお聞きした後に調べていたところ，プライバシー影響評価が，今回の個人情報保護法では事業者に求められなかったというようなことのようですが，この辺りの意義といいますか，ＯＤＲに関して先生の御見解をお聞かせいただければなと思っております。

抽象的な質問で恐縮ですが，よろしくお願いいたします。

○湯淺教授　どうも御質問ありがとうございました。

御質問いただきましたように，ＮＣＳＬでは，州裁判所の裁判手続のセキュリティー，あるいはＯＤＲ等のセキュリティーについても支援を行っております。

御質問を頂きましたように，アメリカの特色は，比較的第三者による認証の活用，あるいは第三者によるレビューを受けることの活用という点にあろうかなと思います。実際，私の領域で申しますと，例えば，州政府が特定の事務については，アメリカの場合だと郡，カウンティ等にセキュリティーコンサルタントのレビューを受けることを，カウンティに対して州政府が義務づけたとかというような事例もあったりいたしまして，そういう外部の専門家の活用というのがアメリカの特色なのかなと思っております。

そういう意味で言うと，本当は日本も司法に関する全般的な第三者機関が，例えば，日弁連の下などで第三者的な機関を本当置かれると望ましいのかもしれませんが，現時点ではまだちょっとそこまでいっていない状況ですので，じゃ，どうするかということで，御質問にありましたＰＩＡでございますけれども，これは，日本ではマイナンバー法を導入した際に，マイナンバーを取り扱う行政，あるいは地方公共団体等についてはＰＩＡを行うことが義務づけられております。地方公共団体の場合には，さらに，ＰＩＡを行うだけではなくて，それを第三者に点検を受けることが義務づけられている現状でございます。

私も幾つかの地方公共団体のＰＩＡの第三者点検に関わらせていただいておりますが，やはり相当大変な作業であることは確かです。どんな事務システムを持っていて，そこにどんな項目の情報があって，どういうネットワーク構成になっていて，さらに，そこから漏れるリスクはどれぐらいで，リスク対策はどうなっていて，業務委託先はどこで，再委託は禁止

しているのか，していないのか，再委託するとすれば，それは文書で許諾なのかとか，非常に多々な項目がございます。したがいまして，個人情報を取り扱う事業者全てに，そういうＰＩＡを求めるということは，特に中小事業者には非常に負担になるということから，現状では個人情報保護法上，民間事業者全体にＰＩＡを求めるところまではいっていないということなのかなと思っております。

しかしながら，ＰＩＡ，特定個人情報保護評価，マイナンバーのＰＩＡ自体は様式が個人情報保護委員会のサイトにございますので，そちらも御参照いただければと思いますが，それを，例えば，もう少し簡略化したようなもので，ＯＤＲ機関にＰＩＡをお願いするというようなことは，先ほど御紹介をさせていただきましたリスクの評価という点では，非常に役立つのではないかなと思っております。

○渡邊委員　ありがとうございます。

○垣内座長　ありがとうございます。

では，川口委員からお手が挙がっていますので，川口委員，お願いします。

○川口委員　川口でございます。

湯淺先生，大変貴重なお話，どうもありがとうございます。

１点，１７ページのところで，先ほど佐成委員からの御質問に対して御返答いただいたクラウドサービスの件について，１点お伺いしたいことがございます。

国内にあるか，海外にあるかということによって，その対応が違うということで御説明がございましたけれども，民間事業者からは，サーバーがどこの国にあるのかということを教えてくれないケースがあるかと思われます。そういった場合，確認する方法とか注意すべき点とか，そういったものがございましたら，教えていただけたら有り難いです。どうぞよろしくお願いいたします。

○湯淺教授　どうもありがとうございました。

御質問いただいた点が，正に今，クラウドサービス利用上の問題点の一つなんだろうと思います。どこの国のどのサーバーにデータを置いているかということは，事業者にとっては，逆にある種の営業秘密になっている部分もありましょうし，なかなかやはりそれは，事業者は明示したがらない。ですので，逆に，先ほど申し上げたような，国外にデータが置かれることのリスクを考えるのであれば，逆に向こうから明示的にわが社のクラウドサービスは国内にデータセンターを置いています，データを置いていますというところを選ぶしかないというのが現状でございます。

あともう一つは，今，ＡＷＳ等に限らず，米国，アメリカ発のサービスがクラウド業界を席巻している状態にありまして，全く純国内だけのサービスを選ぼうとすると，非常に選択肢が狭くなってしまいます。したがって，これはある程度クラウドを利用する上での，現在の制約でやむを得ないと考えざるを得ない部分もあるかなというのが現状でございます。

○川口委員　どうもありがとうございました。

○垣内座長　どうもありがとうございます。

なお，ほかに御質問等，更にございますでしょうか。

あるいは，委員以外のオブザーバーの皆様でも，御質問がもしおありであれば，お申し出いただければと思いますけれども，特段ございませんでしょうか。よろしいですかね。

そうしましたら，湯淺先生には，大変貴重な御講演に加えて，大変多くの御質問に丁寧に

お答えいただきまして，誠にありがとうございました。重ねて，心より御礼申し上げます。

湯淺先生は，本日終了までおいでいただけると伺っておりますので，あるいはまた，後ほどお教えを請うことがあるかもしれませんけれども，よろしくお願いいたします。

どうもありがとうございます。

○湯淺教授　どうもありがとうございました。

○垣内座長　それでは，続きまして，議事次第の３に進みたいと思います。

こちらに関連して，斉藤委員から資料を御提供いただいておりますので，斉藤委員から資料３について御説明をお願いしたいと思います。よろしくお願いいたします。

○斉藤委員　委員の斉藤睦男です。

これは，２０２１年１月末時点のものです。アンケートの集計方法としては必ずしも見やすいとは言えないんですが，実務の実態が分かる情報が非常に少ない中で参考になると思い御提供した次第です。

九つの弁護士会から回答が寄せられています。このうち，福岡県弁護士会は，認証ＡＤＲの一つで，変更認証の申請前の準備段階における回答ということで御理解いただければと思います。

さて，かなりの質問項目があって，これ全部やると時間がなくなりますので，大きく１０ぐらいの項目について解説をしたいと思います。

まず１番目として、第１の１をご覧ください。規則の改正をしたか，しなかったかについては，したところとしないところに分かれていますが，もともとの規則がどうだったかにもよるので，そんなに大きい意味はないかなと思います。

次に二つ目としては，第１の２のところです。これはちょっと面白い質問だと思います。リモートＡＤＲ，すなわちオンラインＡＤＲは飽くまで例外という位置づけなのか，それとも，現実の出頭と同等に扱うのかという，これはリモートＡＤＲの位置づけに対するスタンスないしポリシーの問題ですね。福岡県弁護士会だけが，リモートＡＤＲは飽くまで例外であって，リアルでの実対面方式が原則なんだという位置づけをしています。大事な問題なので関心持っていただけると良いと思います。

では，三つ目にいきますが，第３のところをご覧ください。リモート選択のイニシアティブの質問があります。これに対して，第３の１，これは申立て段階ですが，東京弁護士会の回答を御覧ください。申立人は申立書でオンライン期日を希望することができ，相手方も応諾するに当たりオンライン期日を希望できる。これが多分，申立て時点ないし応諾時点での実務の運用における一般的な扱い方ではないかなと思われます。

次のページを御覧ください。

今のイニシアティブ問題のまとめの６の質問項目で，上記１ないし４の制度とした趣旨・理由を尋ねています。ここも，東京弁護士会の回答を御覧ください。オンラインによる期日が相当であるかは事案ごとに異なるため，当事者の意思を尊重しつつ，あっせん人が判断することとした。これが，平均的，ないし一般的な考え方ではないかなと思います。

その中で，第二東京弁護士会が，３番と４番の解答欄の中に，誰がイニシアティブを取るにしても，双方当事者及びあっせん人の全員が合意した上で行っているという回答をされています。実際の運用はこういうふうになるんだろうと思います。

３ページに移ります。

第５，申立ての方法のところです。１番の，紙媒体によらない申立てを認めない，認めるという項目について，第一東京弁護士会と第二東京弁護士会は認める，つまり，オンラインの申立てを認めるという体制になっている。ただし，実際にそれが運用として既にできているかどうかは分かりません。ほかの弁護士会は紙媒体を主体にしているようですが，東京弁護士会は検討中，それから，右の方にいって岡山弁護士会も仙台弁護士会も検討中ということで，オンライン申立てについてかなり検討が広がりつつあることが読み取れます。

さて，また少し飛ばしまして，次のページ，４枚目にいきます。

上から二つ目の質問項目，期日における当事者の所在について何か制限があるか，無制限かという質問項目について，八つの弁護士会は制限はないです，当事者はどこにいてもいいですと回答しているのに対し，福岡県弁護士会は，非公開性が確保されている場所に限定しますという回答をされています。これも注目される点かと思い御紹介しました。

それから，同じページの下の方の第８，本人確認の方法についてに移ります。何時，誰が，どのように確認するか，これについては，多くの弁護士会が身分証明書を提示してもらうという回答になっております。

その次の第９，非公開・秘密保持についての質問が，次のページにかけてあります。２番，３番，４番，５番を順に見ていきます。２番は，期日の録音・録画・生配信，第三者の無断同席等を防止する方法として，九つの弁護士会が全てそれを禁止する旨の注意を行っていますと回答しています。

そして，３番，リモートによる期日開催によって情報漏えい等の事故が生じた場合に，会を免責する旨の同意を書面で取り付けていますかという質問に対しては，９分の３が取り付けているという回答を寄せています。

４番目の、誓約を書面で取り付けているか、については，９会のうちの４会が誓約書を取り付けているということです。

そして，５番目の，無断録音・録画などがなされた場合の当事者に対するサンクションがあるか，ないかについては，定めていない，あるいは今後検討するという回答になっております。

このページの一番下の第１１，和解のところの２番を御覧ください。

質問項目として，リモート期日で成立した和解について，和解契約書への署名押印の方法が尋ねられています。これについてのこの時点の回答は，やはり郵便でやりますという回答が圧倒的に多いですね。持ち回りになると思うのですけれども，和解契約書を紙媒体で作成して，それを郵便でやり取りしますということになっています。

一番右側の仙台弁護士会が，この回答時点でもそうだったんですが，回答の欄の後半の方に，メールや録音・録画を併用して意思確認を行うことで，署名押印に代える方法が実施可能なように，手続細則を改正済みと書いています。これはどういうことかといいますと，紙媒体で郵便で和解契約書の署名押印をやっている最中に，当事者の心変わりが発生したということがあるんです。つまり，全面的な心変わりじゃないにしても，この和解条項をこういうふうに修正してほしいという要望が後から出てきたことが，仙台弁護士会であったようです。こういうことは，対面だったら案外少ないです。きちんと和解条項を読み上げて，これでいいですねと面前で確認すれば異論はまず出ないし，微修正が必要であればその場ですぐ直して署名押印をしているからです。和解契約書を郵送で持ち回りしている段階で修正要求

は，リモートＡＤＲならではの事態かなと思います。

そこで，仙台弁護士会では，二つの改善策を設けています。リモートＡＤＲで和解条項を読み上げたときに，承諾しました，同意しますということを，メールで弁護士会に送ってもらい、それで確認を取って，署名押印に代える方法が一つです。それから，同じく和解条項を読み上げて，それでいいですと当事者が言う場面を弁護士会の方で録音・録画をする方法も設けました。さらに進んで電子署名という方法がありますが、それはやっていませんということでした。

次のページの第１５をご覧ください。２０２１年１月時点の実施状況が書かれています。東京弁護士会が１件中１件やりましたと回答していますが，これ，実は，私が相手方代理人で，是非リモートでやってくれと東弁に頼んで実現したケースです。ほかに，一弁が１０件中８件，二弁が６２件中２３件，それから，一番右の仙台弁護士会は，リモートＡＤＲの開始が早かったせいもありますけれども，１２８件のうちの２７件ということで，リモートが利用されている状況が分かります。

第１６，これもなかなか興味深い質問だと思います。質問項目は，リモートによる手続の質的変化についてです。当事者のあっせん人・調停人に対する信頼感や手続に対する満足度の低下，あっせん人・調停人の手続実施上生じた支障など、手続の質的低下・変化等を聞いています。これに対して，技術的な面，ないしシステム面での不都合，不具合があったという報告がありますが，それと併せて，京都弁護士会から，リアルのあっせん手続と異なり，ウェブ調停は肌感覚がないという回答，それから，表の右の方の岡山弁護士会から，直接当事者と接しないために，当事者の微妙な感情の機微を感じ取ることが難しかったとの意見があったということを紹介されています。

私も，実は仙台弁護士会で２件ほどリモートＡＤＲの仲裁人，すなわちあっせん人をやっております。つい最近，あっせん人をやった事件で，解決金額についての対立がありました。申立人が請求する側で１００万円を請求していましたが、５０万円でも良いという申立人の譲歩案が出ました。申立人は，この自分の譲歩案をのんでくれなければ不成立でいいです，もう裁判やりますというお話をされていました。相手方にこの譲歩案でどうかと聞いたところ，いや，それでも駄目ですと，相手方としては１０万円がギリギリなんですという回答です。その答えを申立人に伝えました。そうすると，申立人は，じゃ，もう裁判だといきり立つのかと思ったら，違うんですね。ちょっと下を向いたんです。ちょっと下を向いて，何か自問自答している様子がうかがえました。そこで，私の方から，気持ちの切替え料として１０万円ということも考えられますねという話をしたら，ぱっと顔を上げて，分かりました，それで決めてくださいという回答が来ました。

これ，実は，相手方はリモートだったんですが，申立人は実対面で、私と同席で話をしていました。これ，もしかすると，申立人もリモートで画面を経てだったらそうはならなかったかもしれません。申立人がうつむいたときに，同じ場にいたので自分と対話をしているような様子がリアルに感じ取れましたが，画面だったらそこに気が付かなかったかなという，そういう経験をしました。

ということで，私からの紹介は以上ということになります。

○垣内座長　どうもありがとうございました。

それでは，ただいまの斉藤委員からの御発表につきまして，御質問あるいは御意見等おあ

りでしたら御発言を頂ければと思いますが，いかがでしょうか。

出井委員，お願いします。

○出井委員　斉藤先生，どうもありがとうございました。

私からは質問を２点，確認的な質問になるかと思いますが，まず，今回御紹介いただいた弁護士会でのリモートＡＤＲのいろんな問題状況，どういう形でやっているのかと，どういう問題が出ているのかということですが，弁護士会のＡＤＲですから，期日を設けて，本来対面でやっていたものを，コロナ禍だということもあって，ウェブ会議とか，場合によっては電話会議に切り替える，それも，当事者双方がウェブ会議の場合もあれば，先ほど最後に紹介されたように，一部当事者だけはリアルで対面，他の当事者はリモートであると，そういう形態でのＡＤＲ，和解あっせんという理解でよろしいですね。つまり，ＯＤＲ活性化検討会，さらに当検討会の対象でもあるチャットベースで，期日とかいうものを設けずに進めていく形のＡＤＲ，それはまだ弁護士会ではやられていないという想定でよろしいでしょうか。それが質問の１点です。

それから，もう一つはもう少しスペシフィックな質問で，第５の申立ての方法のところで，紙媒体が中心だということでしたか。すみません，その紙媒体の意味なんですけれども，これは，実際に紙を持ち込む，あるいは郵送という意味なのか，ファクシミリはどうなのか，紙媒体によらない申立てというのは，つまりｅメールでの申立てのことなのか，ちょっとそこを確認していただければと思います。

○斉藤委員　第１点目は，チャットベースは念頭にないというか，どこもまだ考えていません。やはり画面を通してやるということをリモートＡＤＲと称しているということになります。

申立てに関しては，このリモートがなかったときは，紙媒体で，申立書を作成して郵送するか，弁護士会の窓口に持ってくるかという方法になっています。多くの弁護士会は多分，災害ＡＤＲの場合はともかく、ファックスによる申立は認めていないだろうと思います。やはり直接持ってくるか郵送でと。それを，リモートＡＤＲを機にオンラインでの申立てもできるようにしている弁護士会がないかというのが，第５の１の質問の趣旨でありました。それを認めているところは，この時点ではなかったのですが，オンラインによる申込みも可能にしようということを検討している弁護士会が幾つか出てきてはいます。

○出井委員　ありがとうございました。御質問に対する御回答は分かりました。

ちょっと一言だけ，最後に斉藤先生が紹介された，１００万とか５０万とかいうのは，多分架空の数字だとは思いますが，実は私も最近同じような事例を経験して，斉藤さんと逆で，ちょうど同じような状況で，申立人はやっぱりリモートだったのですが，結局斉藤委員のような展開にはならず，打切りになりました。やっぱりそこは，リモートの場合，そういう状況で更に申立人に対してプッシュするのか，もう一押しというのはなかなか難しかったというのが印象です。

その１件だけなので，他の事例でどうかは分かりませんが，斉藤先生のお話を聞いて，やっぱりリモートとリアルは違うところがあるんだなと思いましたので，一言だけ。

○垣内座長　ありがとうございます。

それでは，ほかの委員の先生方から，何か御質問等おありでしょうか。

上田委員，お願いします。

○上田委員　ありがとうございます。

ちょっと教えていただきたいことが１点ございます。

斉藤委員に，弁護士会ＡＤＲの実態につき，大変貴重な御教示をいただきまして，ありがとうございます。

頂いた資料の５ページになるでしょうか，第９の３の部分に関してなんですけれども，先ほどの湯淺教授の御講演にも若干関係することかなと思うんですけれども，今後，民間のＡＤＲ，ＯＤＲ業者などが，情報漏えいについてあらかじめ免責条項を定めるということもあろうかと思うのですけれども，ここについて，消費者契約法８条の免責条項の問題もあろうかと思います。当事者がどういう属性かによっても変わるかもしれませんけれども，この点について，どういう御対応をされているのかって，もしお分かりのことがあれば御教示いただければ幸いです。よろしくお願いいたします。

○斉藤委員　御質問ありがとうございます。

消費者契約法８条については私も頭に引っ掛かっていたのですが，免責条項が具体的にどういう内容になっているのかまでは点検していません。多分、弁護士会のことですから，消費者契約法は意識してクリアできるようにしているとは思うんですけれども，ちょっと今は御紹介できません，申し訳ないです。

○上田委員　ありがとうございます。

○垣内座長　どうもありがとうございます。

小澤委員からも挙手があるようですので，小澤委員，お願いします。

○小澤委員　斉藤先生，ありがとうございます。貴重な御報告，大変参考になります。

１点教えていただきたいのが，第１１の和解のところなのですが，和解成立後に，実際紙でということが多いというように，このアンケート結果を拝見しましたが，電子署名を活用されているセンターなどはおありになるのでしょうかということが，お聞きしたいことです。

以上です。

○斉藤委員　電子署名を活用している弁護士会はないですね。今後はあるかもしれませんが，現時点ではない。その手前といいますか，先ほど紹介しました仙台弁護士会でやっているやり方を前段階の方法と呼べは，そういう方法を考えている弁護士会はあるとは思います。

仙台弁護士会に電子署名やらないのかと委員長に聞いてみたら，いや，そこまではちょっと考えていないと。便利だからといって方法を特化してしまうと，汎用性が損なわれてしまうので，汎用性のある段階でとどめた方がいいんじゃないかという回答がありました。御参考までにお伝えします。

○小澤委員　ありがとうございました。

○垣内座長　ありがとうございます。

そのほか，さらに御質問等おありでしょうか。よろしいですかね。

もしないようでしたら，私の方からも，念のための確認というか，１点ですね。

今，オンライン，リモートということで御紹介のあった手続というのは，ウェブ会議等を使うということだと思うんですけれども，従来，弁護士会のＡＤＲでは，一方ないし双方の当事者が電話で参加する形での期日を行うということは，基本的に行われていなかったという理解でよろしいんでしょうか。他の分野のＡＤＲでは，そういう例もこれまであるように思いますけれども，その点，御確認の御質問となります。よろしくお願いします。

○斉藤委員　電話の利用はないわけではないですが，具体的にどういう実績があったかまでは

報告できません。これに対し，テレビ会議システムを使って期日をやるということは，それほど珍しくないと思います。特に金融ＡＤＲでは，被害者の申立人が地方にいて，相手方の金融機関や業者が東京にいるような場合に，地方と東京の弁護士会をつなぐテレビ会議システムがよく利用されているということは聞いています。

一般のＡＤＲの場合でも数は少ないですがテレビ会議の利用は行われています。これは身近にあった例ですが，ＡＤＲセンターが岩手弁護士会で、申立人は岩手だが，相手方が宮城でした。相手方は，盛岡まで行きたくない，仙台でだったら参加してもいいというリクエストを出してきたので，それじゃ，仙台弁護士会と岩手弁護士会をテレビ会議でつなぐから，仙台に来て下さいと，そういう仕組みを作ったということがあります。

そのような状況です。

○垣内座長　どうもありがとうございます。

○出井委員　ちょっとよろしいですか。

○垣内座長　はい，どうぞ。

○出井委員　出井です。

斉藤委員の御発言に補足しますと，斉藤委員からも御紹介あったように，金融ＡＤＲ，これは結構，隔地者間のＡＤＲもそこで行われることもあり得るという想定ですので，金融ＡＤＲにおいては，電話会議を使うこともあると思います。ただ，テレビ会議も結構多いということですかね。

それ以外の，例えば，東京の当事者だけのＡＤＲで，電話会議をこれまで使ったかというと，今はコロナ禍なので，そういうのもウェブ会議でやっているわけですが，その前は余りそれは，それが駄目だということもなかったのかもしれませんが，実例はほとんどなかったのではないかという理解です。金融ＡＤＲ以外はですね。

○垣内座長　分かりました。どうもありがとうございます。

それでは，山上課長お願いします。。

○山上審査監督課長　斉藤先生，ありがとうございました。

事務局からで大変恐縮ですが，１点ちょっと，拝見していて意外な感じがした回答がございまして，それが，第９の１になるんですが，当事者の居場所に制限があるかどうかというところで，ほとんどの弁護士会ではないという回答でした。

先ほどの湯淺先生のお話との関係で言えば，当事者に対してどれぐらいのセキュリティーレベルを求めるのかというお話との関係かと思うんですけれども，従前の対面の弁護士会のＡＤＲであれば恐らく，密室とは言わないまでも，第三者からは隔離された状態でされていたと思うのですけれども，それに対して，ウェブ会議型のＯＤＲの場合には，特にそういった点について当事者に求めていないというところは，どういった背景事情があって，こういう結果になっているのかという点，もし斉藤先生御存じでしたら，教えていただけますでしょうか。

○斉藤委員　個人的な回答になりますが，そうですね，リモートの利便性を優先させているのではないかと思います。いつでもどこでも参加できますよといううたい文句で，リモートＡＤＲを導入し，誘導をしているわけですので，どこにいてくださいとか，どういう条件でないとリモートが使えないんですとか，そういう制約的な方向のアナウンスはなされていないので，こういう結果になっているのかなと思います。

ただ，今日のお話を聞きますと，ここはやはりある程度考える必要がある問題だなというのははっきりしましたので，更に少し考えてみたいなと思います。

○山上審査監督課長　どうもありがとうございました。

○垣内座長　どうもありがとうございます。

オブザーバーの方で，森大樹先生，手を挙げておられますか。

○日本弁護士連合会　日弁連からオブザーバーで参加しております森と申します。

先ほどの山上課長の御質問に関連して，私も，第一東京弁護士会の方で，この制度の仕組み作りを担当しておりましたので，一例ということで御説明申し上げますと，確かに，場所的に制限はしておりませんが，私どもの場合は，次の質問を見ていただくと分かるんですけれども，第三者の方の同席というものは禁止させていただいております。したがいまして，実務的に，もし接続テストですとか，本番のときに，例えばカフェだとか，そういうような不特定多数の方からのぞけるような場所から接続された場合については，そのときにお断りをするとか，第三者の同席，同席というのかどうか，ちょっと分かりませんけれども，そういったことについては制約させていただいているつもりです。

したがいまして，物理的に，例えば，自宅ですとか事務所でなければいけないだとか，そういうような形での制限は設けておりませんが，実質的には，機密性の確保できるような場所というか，環境は確保していただくというのは，当事者双方にお願いしているつもりでございます。

以上です。

○垣内座長　どうもありがとうございます。

では，続きまして，出井委員，お願いします。

○出井委員

今，森さんの補足で十分足りていると思いますが，どの弁護士会ＡＤＲも，非公開であるというのは決められていると思います。

多分質問の仕方によるでしょうが，場所について，特段の規則上の限定はないというお答えではないかと思います。例えば，弁護士会でなければいけないとか，どこどこの会議室でなければいけないとか，そういうことはないと。

ただ，今，森さんからもあったように，非公開の手続ですので，カフェでやったりとか，そういうのは，それはやめてくださいということに恐らくなると思いますし，実務上も，私も何件かリモートでやりましたけれども，両当事者に，今どういう環境で参加されていますかと，周りに誰もいませんねということを，必ず手続の冒頭で確認するようにしていますし，それから，会社の場合は社内なのでいいとはいえ，会社のほかの人がどんどん出入りするような場所，そこはちょっと避けてくださいと。会社内なので，それでも問題ないといえば問題ないのですけれども，やはり相手方のことを考えると，いろんな人が出入りするところは避けてくださいということで，別の会議室に移動していただいたこともございます。

それから，個人の居宅の場合にも，これ，家族が後ろで映り込んだりすることはあるのですが，やっぱりそれも，それはプライバシーが見えてしまうという面もあるし，やはり当事者ではない人，家族であれ当事者と違う人が入ってしまうということもあるので，そこは，そういう環境ではないところを確保してくださいということをお願いするようにしています。

そういう配慮はしているということで，ここは恐らく，規則上限定がないと御理解いただ

ければと思います。

○垣内座長　詳細に補足を頂きましてありがとうございます。

大体，斉藤委員の御紹介いただいたアンケートについては，この辺りでよろしいでしょうか。

それでは，斉藤先生，どうもありがとうございました。

○斉藤委員　ありがとうございました。

○垣内座長　ちょっと時間か押しておりますけれども，いかがいたしますか。

すみません，ちょっと進行の，私の方で不手際がありまして，時間が大分残り少なくなってまいりましたけれども，本日，さらに資料１について事務局から御説明を頂きたいと思いますが，その後，この資料１についての討論のための時間を，今日時間内に取ることが難しいと思いますので，議論については次回にお願いしたいというように考えます。申し訳ありません。

それでは，事務局から資料１について御紹介をお願いいたします。

○渡邊参事官　それでは，資料の１を御覧ください。

時間の都合もございますので，本日は，資料１の作成の趣旨についてお伝えした上で，内容についての御意見は，次回お伺いしたいと思います。

前回の検討会でございますけれども，第１フェーズの推進のための規律の見直しなどの議題で，委員等の皆様から幅広い観点からの御意見を賜ったところでございます。本日以降は，前回の御議論を踏まえつつ，第１フェーズ，第２フェーズにおけるＯＤＲの推進に向けた課題ですとか，その解決策について議論を進めてまいりたいと考えておりました。

デジタル時代を迎えまして，国民の紛争解決ニーズは一層多様化するものと思われ，紛争解決手段の選択の目安となる民間ＡＤＲの認証制度が果たすべき役割機能は，ますます重要なものとなると考えられます。前々回の渡邊委員の御講演では，ＡＤＲにデジタル技術を活用するに当たっても，現在の紛争解決手段にどのような課題があるのか，その解決のため，どのような技術をどのように活用していくべきなのかというアプローチが重要であるという御指摘がありました。

したがいまして，まずは，ＯＤＲをどのようにデザインしていくのか，目指すべきＯＤＲについて議論を深め，認識の共有を図っていく必要があろうかと考えております。その上で，選択の目安として認証されるべきＯＤＲの具体像を描き，現行の規律について課題を洗い出して，解決策の検討を進めるべきであろうと考えております。

こうしたコンセプトに基づきまして，ＯＤＲの公正，かつ適正な実施を確保する上で生じ得る課題を念頭に置きつつ，現行の認証の基準・要件や認証紛争解決事業者の義務に関して，検討すべき項目について論点例を挙げつつ，その全体像をお示ししたと，こういう次第でございます。

事務局としましては，主に検討すべき項目として７項目を挙げましたけれども，それ以外の項目を排除する趣旨ではございませんし，他に検討すべき項目があれば，皆様の御意見を賜りたいと存じます。

資料作成の趣旨は以上でございますので，次回，この点について御意見あれば伺いたいと思っております。

以上でございます。

○垣内座長　どうもありがとうございます。

そのようなことで，今後検討されるべき課題の全体像をお示しするという趣旨で，論点を種々挙げていただいているということで，次回以降，これらの論点について，あるいは，更に加えるべき論点があれば，それについても是非積極的に御意見を頂きたいということですので，引き続き御検討をお願いしたいと思います。

よろしいでしょうか，今の趣旨につきましては。

どうもありがとうございます。

そうしましたら，ちょうど時間になってまいりましたので，本日の審議につきましてはここまでということにさせていただきたいと思います。

本日は，湯淺先生，また斉藤委員から，大変貴重な御講演，情報提供を頂戴いたしまして，今後の議論にとって大変有益な御示唆を頂けたのではないかと考えております。

湯淺先生には，改めまして心より御礼申し上げます。どうもありがとうございました。

○湯淺教授　どうもありがとうございました。

○垣内座長　そうしましたら，事務局から今後の日程等について御説明いただければと思います。

○渡邊参事官　次回，第１０回の会議は６月３０日水曜日の午前１０時から正午まで，場所は法務省赤れんが棟の３階の第四教室を予定しております。引き続きウェブでの参加もお待ちしておりますので，御協力のほどよろしくお願いいたします。

詳細は後日，また事務局の方から御連絡をさせていただきたいと思います。

以上です。

○垣内座長　ありがとうございます。

それでは，本日の会議はこれで終了といたします。

本日もどうもありがとうございました。

－了－