裁判手続等のIT化検討会（第６回）議事要旨

日　時：平成30年２月22日（木）８:28～10:36
場　所：中央合同庁舎第８号館５階共用会議室Ｂ

１．議事
（１）情報セキュリティ対策について
（２）事務局説明
（３）自由討議

２．「裁判手続等のIT化にともなうサイバーセキュリティについて」（資料１）デロイトトーマツリスクサービス株式会社北野パートナーより説明。

- 北野パートナー
  裁判手続等のIT化を検討するにあたりシステム構築をどのようにするか、システムや組織のサイバーセキュリティをどのように考えるか、考えをまとめてきたのでお話ししたい。
- 資料だが、まず一旦、基本に立ち戻り、あらゆるシステムとか、あらゆる業務とか、そのようなものをIT化するときにセキュリティについてどう考えるのか、少し整理した。端的に言うと、何を守るのか、何から守るのか、どのように守るかという話。それに加えどのぐらいのレベルまで、どの程度守るかということ。これらを今回の裁判手続をIT化する際にどのように考えていくかということ。
- 順番に説明すると、何を守るのかはよく情報セキュリティの世界でCIAと言われる。機密性、完全性、可用性と呼ばれるが、一般的に漏えいしない、改ざんがされない、失われない。「失われない」（可用性）はシステムが止まらないことも含めて、情報を使いたいときに必ずいつでも使えるようにしておくことだが、これらを考えたときに何を守るのかを考えるべき。我が国の議論は、どうしても個人情報漏えいみたいなものがニュースで取りざたされることが多いため、やや機密性に偏った議論が行われていることが多いと感じているが、実際には考えるべきことはそれだけではなく、情報が正しい状態であることを守らなければいけないとか、情報システムがとまらない、情報がいつでも使えるようにしていかなければいけないといったことも守らなければいけないものの１つだと考えられる。
- 機密性については、いずれのシステム、いずれの業務についても、どんな情報を取り扱うのかをまず整理する必要がある。いろいろ資料等を見て、今回取り扱われる情報の中で機密性の高いものはどのようなものだろうかと、考えてみたが、このように情報を分類してみることが必要である。資料では政府統一基準の例を１つ吹き出しの中

に挙げている。専門的にはクラシフィケーションと言うが、情報を分類した上で機密性のレベルを決めて、では機密性の高いものはどれぐらいのレベルまで守るのか、ないしは公開範囲をどうするのか等を考えていくことで、当然、機密性の高いものほど問題が起きたときのインパクトは大きくなるから、リスクは大きい。このように考えていく。まずここを整理する必要があると考える。

- 裁判手続の中では情報が改変されると問題がいろいろ全体の中では起きると想像するわけで、これは守っていかないといけないだろうと思う。ただ、万が一、改ざんがあっても手続の過程のどこかでわかるのではないか。最終的に紙を使った証拠調べの手続もあるという話を聞いたわけだが、一応、改ざんというものがどこかで発覚、検出できると思われる。従って、恐らく今回この手続のシステム化をしたときに、その情報、紙とかデータとかではなくて、中に入っているコンテンツそのものの情報といった意味では、改ざんされたままの状態であり続けたり、失われたりすることはないのではないかと思う。つまり、もともとは紙で情報としてあったものが、どこかの段階でコンピュータに入力されて、システムの中で取り扱われているから、最終的に紙を使った手続もあるということなので、どこかで検出できる、そのように考えながらシステム化を考えていく必要があるのではないか。
- 最後の可用性について、これは後々の「どれぐらい。どの程度まで」という部分にも出てくるが、実際にもちろん無くなってはいけない。これもシステムだと、バックアップをしたり、二重化を行ったりすることで、電子的なデータが無くならないようにいろいろな手を打つわけだが、最終的に例えば電子的なデータが消えた場合を考えたときも、今回のケースについては結構紙の情報が残っていることが多いのではないかと思う。ということは回復ができるのではないかと考えている。もし何らかの形で回復ができる見込みがあるのであれば、どれぐらいのコストをかけて、どれぐらい可用性を追求するのかに関係するので、それを踏まえて議論していく必要がある。このようなものをどのくらいまで、どのように定義をしていくのかが今後、整理していく必要が実務的にはある。これが何を守るかということ。
- 次に、何から守るか。昨今、2020年に向かって海の向こうからサイバー攻撃があると専ら話題になることが多いわけだが、脅威はそれだけではない。必ず内部関係者による不正ということも考えなければいけないし、最も多いのは実は人為的なミスである。
- 確かにサイバー攻撃というのもある。参考までに、サイバー攻撃をしてくる相手、攻撃者の類型のようなものをサンプルとして表示している。これは攻撃者にとってのインセンティブの問題にもかかわってくる。最近だとどうしてもサイバー攻撃をする人、犯罪者であったりするわけだが、非常に多いのは経済的利益を求めて攻撃をする。何かを盗む、お金を直接盗むとか、お金になりそうな情報を盗む。売ればお金になるような情報を盗むことが多い。それ以外ではどちらかというと思想信条で攻撃をしているものが多い。

- 今回、何から守るのかを考えるとき、どれぐらい攻撃してくるのだろうかということを想像しないといけないわけだが、攻撃者というのは当然、何か儲かることがある、インセンティブがあるから攻撃するわけで、攻撃者の動機、モチベーションがどこにあるのかを考えていく必要がある。
- 今回のIT化では、例えば仮想通貨の取引所を攻撃してくるような人たちがこのシステムを攻撃してくるだろうかと考えると、そこまでのインセンティブがあるだろうかとか、例えば国家的な攻撃がこのシステムにどれぐらい想定されるだろうかとかを、冷静に考えていく必要があると思う。一般的に多くのサイバー攻撃の事例を見てきた感覚からすると、意外とそんなに大きなインセンティブはないのではないかとも思う。
- 内部関係者についてはいろいろな関係者がある。裁判手続にかかわる関係者が誰であるのかは、先生方がよく御存じかと思うが、内部関係者の人が例えば何かこの手続にかかわる情報を盗むとか、壊すといった行為に、何かインセンティブがあるのだろうかというと、そうでもないのではないかと思う。
- 世の中でよく参照されている「セキュリティインシデントに関する調査報告書」というものがある。これはJNSAというNPOで公開しているもので、それによると圧倒的に件数が多いのは人為的なミスとなっている。これは決して忘れてはいけない脅威として考えなければいけない。人為的なミスは表立って攻撃をされてくることとは少しイメージが違うが、いわゆるCIA、機密性、可用性、完全性を侵害するものを脅威と呼ぶわけだが、この大きな脅威の１つとしては考えていかなければいけないということ。
- 実際にどのような情報を取り扱っているのかを整理し、機密性がどれぐらいなのか。つまり問題が起きたらどれぐらいのインパクトがある情報を取り扱っているのかという整理をし、これを誰から守るかを想定することを一度、明らかにしていく必要があると思う。
- どのように守るのか。どれぐらい堅牢なセキュリティをやるのかといった話になると、どうしても技術的な対策をどこまでやるのかが話題の筆頭に大体挙がる。それはそれでこの後の議論の中でも出てくるのだろうかと思うが、我々が通常考えるのは技術的な対策だけで情報が守れるかというと、決してそうではないと思っている。情報セキュリティマネジメントの要素として。業界ではよくISMSと呼んだりするものがある。ISOで言うと27000シリーズというものだが、このようなところでよく出てくるのは、人的対策、組織的対手策、物理的対策、技術的対策と４つのカテゴリに分けて対策を考える。これらをきちんとバランスよくやっていく必要があるということ。この４つの分類の対策をどのようにバランスを取ってやりながら、目指すべきセキュリティをどう実現するのかということ。実際にはこれをきちんと定義していくことで、過剰投資ではないレベル、このリスク、この情報を取り扱うのにこの攻撃を想定して、これぐらいのリスクであれば、これぐらいの対策の内容でいいだろう、といった着地点を見出していく。このようなところを明らかにしていくべき。

- もう一つ、資料ではPDCAをどのように回していくかということも示している。これは何かというと、例えばある時点で非常に強固な技術的セキュリティ対策を備えたシステムを構築したとすると、多分３年も放置したら堅牢なセキュリティのシステムではなくなると考えられる。常に攻撃の手法、攻撃者の側は進化をし、変化をしているということで、３年先の攻撃の手法はがらっと変わっていたりする。
- また、どうしてもソフトウエアとかシステムというのは脆弱性と呼ばれる、後々見つかるバグみたいなもの（弱点）が必ずつきもの。ソフトウエアは必ずバグがあるものだという前提でやっていかなければいけないわけだが、そのような場合に、それに対してどう対応するのかという問題。つまり運用管理をきちんとしていける体制を作る必要がある。そのシステムのセキュリティの対策のレベルをきちんと維持管理し、運用していくという体制と仕組みづくり。これは組織であったり、ルールであったり、運用する人であったりするわけだが、これらがきちんと整わないと、幾ら非常にレベルの高い技術を使った対策をここにインプリメンテーションしたとしても、結果として３年も経つと穴があいたシステムになる可能性が高い。
- そのような問題を考えると、人的、組織的、物理的、技術的というような４つの対策をバランスよく考え、きちんとした技術的にも必要なレベルの対策をしなければいけないが、造ったものを維持管理していく、マネジメントしていくための仕組みづくり、組織づくり、体制づくりを合わせてしていかないと意味がない。
- どれぐらいのレベルまでこの４つの対策をやるべきなのかを、これから考えていかなければいけないのが今回のこの分野のテーマではないかと思うが、前段の何を守るのかという話と、何から守るのかを考えてみると、我々が通常、いろいろなシステムを見ていく中で、軍用とか例えば自衛隊で使っているようなシステムとか、警察で使っているシステムのような比較的高いレベルのセキュリティ対策を実装しているようなシステム、ないしはメガバンクで使っているようなシステム、そのようなところまでセキュリティのためのシステム投資をする必要があるのかは、直感的にそこまでやらなくてもいいのではないかと思う。
- それを指標としてどう考えるかということで、私どもが通常、実務的に使っている業界ごとに目指すべきレベルを示しているが、これは必ずしも絶対的なものではなくて、大体の目安と考えていただきたい。それぞれ細かくは時間がないので説明をしないが、いろいろな対策要素があり、これをだんだん積み上げていくと成熟度が上がってくる。セキュリティレベルとか対策レベルと言わずに成熟度と呼んでいるのは、先ほど説明したように技術的な対策ができているというだけではなく、それがきちんとPDCAのサイクルも含めて維持、管理、運用ができているのか、体制があるのか、人がいるのかも含めて、組織全体で成熟度を上げていかないと意味がないからである。
- この中で実際に先ほど説明したような話を考えると、メガバンクほどではなくてもいいのではないかと考えたというところで、真ん中あたりを一度目指してみるというの

を、仮にこれぐらいかと緑線で囲ってみたところ。

- レベル３とレベル４で、どう違うか、簡単に非常にざっくりした指標を次頁に示している。これもあくまで目安だと考えて頂きたい。例えばメガバンクのシステムは止められないということが大命題としてある。たまに年末年始に計画的にとめることもあるが、そういうことを除いては今や銀行さんのシステムは24時間365日、ほぼ止められないわけで、止まるとどのようなことが起きるかは想像ができるかと思う。
- お金も盗める、止めると社会的に非常に大きな混乱を起こすことができるという意味で、攻撃者に対するインセンティブも非常に大きいと言える。「金融＆通信事業者」と棒グラフに書いているが、例えば大手の通信事業者のシステムが止まったらどのようなことが起きるかを考え、そこまでのものが裁判手続のシステムに必要かを考えていく必要がある。「金融＆通信事業者」の一歩手前、一定の時間は停止が許容できるシステムといった、比較的社会的な影響があるけれども、ある程度対応ができるだろうという仕組み。それから、もう少しレベルを落とすとインシデントの社会的な影響、組織の単位、例えば会社とか、組織の事業にはそれなりに影響するけれども、社会全体がとても困るというほどではないというレベルのような、そのような視点でレベル分けをして、どのあたりを目指すのが一番現実的なのかを考えていく必要があると思う。
- 今までの説明を踏まえて、どれぐらいのことを具体的にやるのか、例示を幾つか持ってきた。金融機関でどのような取り組みをしているのか、日々目にすることも多いかと思うが、銀行だと最近はワンタイムパスワードが流行っていて、イメージを出しているが、スマホのアプリで利用したり、専用のカードを配っているものなどがある。
- もう一つは、銀行のオンラインバンクを利用するときに、例えば海外出張して出張先から使おうとすると、うまく使えないといったことがあるかと思うが、これは通常、日本国内からしか利用していない人が、ある日突然実績のない海外から利用すると、この人は本当に本人かなというような判断（別人によるなりすましではないかという疑い）を自動的にシステム側がして、「あなたが本当に本人だったらもう一つこのパスワードを入れなさい」とか、システムが要求してくるという例。最近はFacebookとかGoogleでも多要素認証を設定することができる。たまにブラウザを変えたり、パソコンを買いかえたり、携帯、スマホ等を買いかえたりすると、初めての端末からアクセスがあったということで携帯電話に番号が飛んできて、それを入れないとアクセスができない、といった仕組みが実装されている。これはよく「リスクベース認証」と言われているものだが、このような認証を使ってなりすましを防いでいる。当然これをやると相応のコストがかかる。我々はソリューションの導入なども支援することがあるが、左側の銀行のワンタイムパスワードとかやろうと思うと結構お金がかかる。それでもリスクがあるので、それぐらいお金をメガバンクはかけているということであろうと思う。

- もう一つ、大事なことがある。なりすましの防止としてどのように認証強度を上げるかに目が行きがちだが、ID管理をちゃんとしていないと意味がない。例えば、もう使わなくなったIDは早く消す、ないしはこの人にIDや権限を与えていいのかどうか。決められた手続を踏んで与える。それを与えたら、それに対して定期的にメンテナンスをする。要らなくなったら早く消す、といった管理。この一連のID管理の手続をきちんとしておかないと結局、要らなくなった人がいつまでたってもID、パスワードの権限を持っていることとなり、３年も経つと幽霊ユーザーだらけのシステムになるということで危険になるので、しっかりと考える必要がある。
- 今回ｅ裁判、e-Court、裁判の実際の公判とかをオンラインで行うことも話題に上っているようだが、ではe-Courtをどのようなインフラでできるのか、最近、私どもも含めて事業会社、民間で使われているものをサンプルとして２つぐらい挙げている。SkypeとWebEX。このようなサービスもそれなりに暗号化を使って盗聴の防止対策も行われているわけで、結構使えるレベルになってきていると考えている。Skypeについては、最近マイクロソフトが「エンドツーエンド」の暗号化をすると表明しているようだ。WebEXはシスコが提供しているものだが、仕様やスペックをさっと見ると、企業向けにつくられているということで結構いろいろな対策ができるようになっていて、割と安全に使うにはいろいろな仕組みが整っているかなと見ている。とはいえSkypeもマイクロソフトが買収してから、Skype for Businessが結構出回っていて、急速に普及している。
- 参考としてどのような暗号技術が使われているかVPN、SSLなどを記載している。いわゆる通信経路をどのように暗号化して盗聴を防止するかという策だが、こういったものが大体普通AESを使いますということでAESを出している。たまに違う暗号方式を使っているところもあるが、おおむねNISTが相当長い時間をかけて選定をして、一定の暗号強度が保証されているということで、このようなものを使っているということである。大体この程度の防止策をやっていると、それなりに機密性の高い企業の内緒の会議とか、社内の余り漏れては困るようなことも、遠隔会議で実際に話をすることができる。このような使い方をしている企業さんも今はかなり多いと思われる。つまりは既存のサービスも十分、現状ないしこれからの利用については検討できる範囲、視界に入ってきているのではないか。このように考えている。
- これまで、情報セキュリティについてざっと説明をした。何から何をどのように守っていくのかということを、一旦整理をしながら議論をしていく必要があるということ。社会的な影響度も含めてリスクがどれぐらいあるのかということを、どのように評価をし、どれぐらいの成熟度のレベルを目指す必要があるのかということ。我々のような立場からすると、過剰な投資は決してお勧めできない。過剰な対策をして利便性を損ねるというのは、もともと今回の議論の中でも実際に裁判にかかわる方、手続をされる方、実際に裁判制度を使われる国民の方々の負担を減らすであるとか、手続を迅速にできるようにするであるとか、そういったメリットを目指してやっていくという

ことだと思うので、一概に利便性を損ねるようなこと、やり過ぎで利便性を損ねるのは本末転倒であり、うまく着地点を考えていく必要があると思う。

- どれぐらいのレベルが裁判に求められるかを今回、私なりに考えたところ、防衛や金融、大手の通信事業者さんのいわゆる356日絶対にとめてはいけない、非常に攻撃者にとってインセンティブのある、攻撃されることがそもそも目に見えているようなシステムに比べると、もう少しリーズナブルに構築してもいいのではないか。そういうことができる可能性の高いテーマなのではないかと考えている。

（委員補足）

- 宮内委員
  今回のこの会議でいろいろ話題になってきた文書のセキュリティとの関係ということで、こういう視点も大事なのではないかということを考えてみたので、参考資料２というメモを見ていただきたい。
- 一般的にいろいろなリスクがあるときに、リスク対応をどのようにやっていくかというものの簡単な説明。何らかのリスクがあるときに、この影響の大きさと発生の可能性というのをマトリックスで考えて、どのような対策をとるかというのが大体ポイントになっている。例えば右のほうで、これは例として挙げたので正しいかどうかわからないが、例えば準備書面をなりすましで出すようなリスクがあるとすると、これはそれなりに影響はあるが、後でばれるのだからそんなことをする人は少ないということで影響度は中、発生可能性は低という具合だ。今言った評価は、大体このようなイメージで捉えていくということであって、低とか中とかの評価が正しいと言っているわけではない。
- このような中で、影響度の中ではいわゆるレピュテーションリスク、こういうことがある。例えば裁判所から漏れたというので全体の信頼性が下がるとか、そのようなものも一応、リスクの影響としては考えるべきだということだ。こういういろいろなリスクを考えて評価していって、左のマトリックスの中にはめ込んでどのような事を検討していくかということを考えていく。こういうことが今後必要になってくるのではないかと考えている。
- ちなみに、左の絵の中でリスクの回避というのは初めから危ないものは持たないとか、そのようなことが裁判所でできるかどうかは別として、必要ないものは消すとかも含めている。右下のリスクの移転は、一般的には保険に入るとかが多いと思う。大体はリスクの低減を行っていって、低くなったらそこは保有していくという形でやっていくと思っている。こういう視点が要るということが１つ。
- 裏を見ていただきたい。それぞれ文書を出すときにいろいろなセキュリティがあるのだが、ここでは先ほど説明いただいたCIAと少し外れたところにある、本人が「私が書いたものではない」と否認するようなリスクも含めて考えるべきではないかというこ

とを説明している。このための技術としては電子署名と認証があって、電子署名は言ってみれば文書に判こを押して出すようなもので、後から第三者から見てもこれは例えば宮内が書いたということが簡単に確認できるというもの。認証というのは例えばID、パスワードみたいなもので、本人を確認しているが、文書そのものは特に署名とかせずに出しているという感じ。

- 右端を見ていただくと、署名のほうは実印を押して印鑑証明を出すようなもの。認証というのはいわばマイナンバーカードや免許証で本人だと確認した上で押印していない紙を渡すようなイメージだ。受け取り手は本人から来たということはすぐ分かるが、後でこの紙が本当に本人から来たのかと問われると必ずしも証明できない。このようにいろいろなレベルがあるということ。このようなレベルを踏まえて検討していく必要があるのではないかと思う。この検討会で細かい議論をやるということではないが、今後検討していく必要がある視点として、御紹介させていただきたい。
- ちなみに、このような内容については、政府でも一番下に記載した電子署名・認証ガイドラインでいろいろと検討されている。こちらも現在、改訂中と聞いているので、それを踏まえてぜひ検討いただきたいと思う。

（自由討議）

- 実際にメガバンクでどのようにしているか参考までにお示ししたい。まさしく銀行は24時間365日、災害のときも止めてはいけないという使命がある関係で、多くのシステムを二重に作っている。例えば関東で大災害があった場合は、速やかに西日本のサーバーで今までどおりの預金取引や為替取引ができるような体制で、かつ、人も24時間365日、常に技術者を待機させていて、システムの稼働を行っているというような非常に重厚でコストのかかったシステムを構築している。まさしく今回の訴訟のIT化においてそのようなレベルのシステムが必要なのかという点については、私は違う世界なのではないかと思っている。
- 認証については、ワンタイムパスワードを参考にお示しいただいたが、資料にも記載のとおり、これはお客様が御利用になる銀行取引の中でも、なりすまされた場合のリスクが高いもののときだけに使う。要するに残高を見るときにはこのようなものは要らない、振り込みをするときには要る、という使い分けをしている。その心は、認証強度を高めるということは結局、利便性を損ねることが今の技術では多い。そのようなことから、銀行の実務においてはリスクの度合いに応じて認証の強度も使い分けている。
- 使いやすさという観点だと、もちろん個人としてのオペレーションの手間という問題もあるが、例えばこのような訴訟などの手続だと、法人としての御利用とか、弁護士事務所での御利用というのがあって、認証というのを個人単位にしてしまうと、法人あるいは組織体で何かを行うというときに、非常に使い勝手が悪いという問題が起き

うる。これは例えば私どもが提供している法人向けのインターネットバンキングサービスなどでも、常にお客様の利便性とセキュリティの強度というところでシステム設計に難しさを感じるところだし、お客様からいろいろと御要望いただくところなので、そこはなかなか難しい問題というか、慎重に考えて利便性を損ねないようにしないといけないと思う。

- Skype for Businessについて。秘密情報をいわば一般ベンダーの提供するシステムでやりとりして大丈夫かということに関しての私どもの取り組みというか状況だが、私どもも同様のサービスを利用している。あるいは先ほど出たVPNという一般公衆回線の中の仮想の専用線を使ったウェブ会議のようなものを実際に行内で使っていて、例えば本邦を代表するような企業の情報というのを我々は日常的にやりとりするわけだが、そういう場合でもウェブ会議を使って良いというルールになっている。その意味ではセキュリティについて、Skype for Businessなど一般的なものを利用するのに心配はないのではないかと感じている。

- デロイト資料のスライドの５ページ、レベル３程度が適当ではないかという１つのモデルを提示いただいている。その真ん中の下から３つ目、入口・内部・出口のセキュリティ監視を24時間365日行うことについて、既に行政機関についてはNISCと呼ばれる内閣官房セキュリティセンターが24時間、常時監視対象にしているが、民事訴訟をIT化する際に裁判所は行政機関ではなく司法権なので、法律上もNISCの常時監視下に入れるたてつけには現在なってない。しかし、それを独立して新たに構築するとなると、非常にコストもかかるので何らかの工夫をして、なるべくコストがかからないようにすべき。実質的に強固なセキュリティ監視体制がとれるように工夫をする余地はないか、と思ったりしているところ。
- アクセス権限の問題は今、企業用のオンラインバンクの口座の難しさの件を指摘いただいた。これは当然、弁護士事務所にも当てはまるし、依頼人と弁護人との関係が変わるということの紐づけと、アクセス権限等をきちんと紐づけする必要があるし、途中から弁護士が変わったときに前の資料を全部きちんと引き継げるかどうか。逆に前の弁護士が辞任した場合に、その後アクセスできないようにするということをどうコントロールするかも、少し工夫の余地があるのかと思う。
- ３番目は、宮内委員提出資料にもあったように、書証の重要度に応じて、単なる事務連絡に近いものにまで、一々電子署名をつけるのは、非常に現実的でない。逆に証拠物については真正性がかなり問われるので、宮内委員に提案いただいたような電子署名の採用も一案だし、いわゆるメタ情報を後から検証できるような仕方が望ましいのではないかと思う。

- ２、３質問をしたい。１つは例えばセキュリティのレベルをネット通販ぐらいのもの、

つまりID、パスワードで使えるという程度でも良いと設計して、しかし、この事件だけはワンタイムパスワードを使わないといけないというような仕組みが作れるかということ。もう１つは、個別事件ではなくて、問題のある事例が随分増えてきてしまったため、IDとパスワードだけではとても全体のシステムが動かない。追加対応でレベルを１つ上げなければいけない。このような対応は非常に大変なシステム改修となるのかどうかということ。そのあたりを教えていただければと思う。

- 北野パートナー
  最初の質問だが、恐らく技術的には実装は可能だと思う。これは先ほど銀行の例で、振り込みをするときだけワンタイムパスワードを使うというような話があったかと思うが、割と似たような実装で、このようなケースだけは違う認証の方式を使うとか、あらかじめ例えばこのケースについては、この事件についてはこのように定義をするという機能を作っておいて、これは非常に慎重に進めるべき事件で機密性が高く、リスクが高いので、「リスク高の事件」であると例えば設定をすると、必然的に例えば２段階認証を要求されるようになるとか、例えばそのようなロジックを作ればいいので、技術的には仕様が決まれば実装は十分可能だろうと思う。
- 質問の２つ目のレベルを上げることについては、技術的にはやる内容によりけりなものなので、なかなか一概には言いづらいものがあるが、なるべく柔軟に変更できるシステムにしておくというのは、設計のときに意識をしておく必要はあるだろうと思う。これは例えばアクセスコントロールのきめ細かさ、どの人にどの情報をアクセスさせるか。これはあらかじめ結構仕様を決めておかないと、後から変えるのが難しい分野だったりするわけだが、それは少し細か目に設計をしておいて、運用するときには緩目から運用する。必要が出てきたら細かい運用もできるようにする。例えばそれを意識した設計にしておくとか、そのようは設計時点での配慮はある程度できるのではないかと思う。

- 参考までに韓国では公認認証書という電子署名の制度があり、もちろんログインIDも別に認証としてあるが、それをログインのときにも利用しているし、加えて提出する書面に公認認証書による電子署名をつけて提出させている形式をとっているようだ。それをつけることが複雑で業務の支障になっている雰囲気はなかった。公認認証書はパソコンに既に入っていて、書類提出のときにチェックをつけるだけで電子認証がつくという形になっていたので、そんなに負担かというと、そうではないと思う。ただ、本人訴訟の場合はどうするのかといった問題は別途あるかと思う。
- あと、日本の訴訟制度に合わせた形でセキュリティリスクの洗い出しをしないといけないと思う。民事訴訟法の92条には、秘密保護のための閲覧等の制限という条文があり、１号では私生活についての重大な秘密、２号では営業秘密といった形で、幾つか

の情報については特に閲覧制限をかけて保護するという立法があるので、情報資産として重要度が高いものについては、それに合わせた保護が必要だと思う。

- それから、性的な被害とか、離婚などの訴訟だとかなりどろどろした部分がある。だから、情報資産の区分けや事件の区分けを行い、情報資産を洗い出してリスクアセスメントする過程が必要で、その過程で法制度と現実を踏まえたアセスメントをした上でセキュリティの設計をしていくことが、いずれは必要になると思う。もちろん、今の時点でそれを細かく議論しても仕方がないと思うが、そのようなことを全体の方向性として忘れてないと付記しておいたほうがいいのかと思う。

- 川村参事官（内閣官房日本経済再生総合事務局）
  昨年ドイツに訪問し意見交換をした際に、ドイツ側の問題意識としてドイツの制度だと紙の場合もその都度、署名をして確認をして記録をしている。それを電子署名で置きかえているような仕組みになっているようで、その電子署名の有効期限があることで、記録の管理でその都度電子署名を更新しなければならず、これが負担であるという問題意識が示されていた。その意味で電子署名を都度都度付すことについて、一見、言葉で言うと簡単だが、実務的に運用すると大変なコストになり得るということは、紹介させていただきたい。

３．「人証調べ・最終口頭弁論期日・判決言渡しまでのIT化の視点」（資料２）、「現行民事訴訟法下における民事訴訟手続の流れの一例（人証調べ・判決等）」（資料３）、について内閣官房日本経済再生総合事務局より説明。

４．自由討議

- １ページ目の（４）のウェブ会議を人証調べに活用することについては、これは今の204条の条文をどのように変えていくのかという検討が中心になると思う。今でも一定の要件のもとで映像等の送受信による通話の方法による尋問は行うことができるので、これをより広く拡大していくことなのだと思う。その方向自体は、私はいいと思っている。
- そのときのやり方については、恐らく今の閉域網ではなく、もう少し広い裁判所以外の場所でもつながるといった話になると思うが、その場合に、その後に書いてある人証調べの（５）、２ページの上の人証調べの公正な実施が担保されるか等との関係では、これは前から出ている、カメラに映らないところに人がいて何か指示をしているみたいなことが一番端的な例だが、そのようなことがないようにするために、どのような工夫が要るのか検討が必要である。
- いろいろなケースがあることを前提にすると、そういう方法をとるかどうかは、現在も裁判所が判断することになっているので、現行規則にある当事者の意見を聞くとい

った手続を踏んだ上での裁判所の裁量で決めていくといった方向が考えられる。ただ、要件が緩やかになって裁量の範囲が広がるとすると、相当かどうかの判断には、より慎重さが求められると思う。当事者の同意がなければ裁判所以外ではウェブ会議をしてはいけないといった仕組み方も恐らく意見としてはあり得ると思うが、そこまで言うといろいろな事案があるのでなかなか対応し切れないとも思っている。

- 最終口頭弁論とか判決言渡しは、憲法82条との関係が問題になって、法廷で口頭弁論期日を開く、あるいは判決言渡し期日を開くということ自体はせざるを得ないように思う。e-Courtなのに形式的なものをそのまま維持するというのは、実質的には何となくおかしな感じもするが、憲法の要請であり、そういう公正さを見せることも大事である。それを前提に、どのようにして、当事者がアクセスしやすくて、双方当事者とも来ていなくても期日としては開ける仕組みにしていくかの検討が必要だと思う。判決言渡しは、法廷に行くのは大変だが、ITの仕組みを利用すればすぐに聞けて便利だという話になるだろう。
- ただ、判決の送達に関しては慎重にやらなければいけない。訴状の送達とは違い、判決の送達については既にずっと手続に関与しているので、アップロードされたデータを見るとか、ダウンロードするとか、そういったことでできるとは思う。ただ、それだけに、当事者本人に伝わる方法でちゃんと送達されたのかといったあたりの仕組みについては慎重に考えなければいけなくて、今、同居者が受け取ればいいという補充送達の制度があるが、そういった補充送達的なものについて、このような仕組みにしたときにどのように考えるのかは、検討課題になると考えている。

- ２の人証調べ手続に関して、裁判の内容によっては対面することが非常に重要であると思っている。レベルが違うが、私の仕事は基本的に電話で聞き取りをしたり、交渉したりということがメーンになっているため、相手の表情が見えないことによって大変難しいところがある。また、ADRにおいても対面で説得をするよりも電話で説得することの方がハードルが高いということは、数々経験しているので、そのような問題があるかと思う。
- 当事者の要請あるいは同意によってウェブ会議を選択することになるかと思うが、裁判官が必要と思ったときにそれを指定できるようなことも必要になるのではないかと思う。特に一般の国民にとっては裁判自体が非常にレアなケースだし、ましてウェブでやるということ自体も人生の中で一度あるかないかみたいな場所になるので、利用するときの事前の心得的なものとか、事前の情報提供あるいは途中での裁判官の説明力の問題になるかと思うが、その人にわかりやすい説明の仕方とか、そういうものが近くで顔を見るとこの人はどのぐらいわかっているのかなというのがおわかりになると思うが、なかなか御表情がわかりにくいとかいった場合のサポートなども、ぜひしていただきたい。

- ウェブ会議は今やられていることを広げるということであって、必要な場合、法廷でやるということは当然だと思う。
- 具体的に考えてみると、対質をする必要がある場合にこれでうまくいくのかという気もするし、隔離尋問を厳格にやらなければいけないというときに、本当に隔離が保障できるだろうかということもある。このような問題もあって、具体的な事件によってはウェブ会議は適当でないことがあろう。もっとも、さらに技術が進んでいけば、そのような場面もカバーできるようになるかもしれない。
- いずれにしても今、不便なものを便利にするという方向でこれを考えていけばいいのではないか。遠くにいて、今は証人になってもらえない人が、ウェブ会議であれば証人になってもらえる。場合によれば外国にいる人は在外公館に来てもらってウェブ会議で証人尋問することだって可能になるかもしれない。
- 鑑定について考えると、これも広がりのある話で、鑑定人には今資料として記録の必要部分のコピーを渡しているが、記録が電子化されれば簡単に鑑定人に資料が渡せるし、鑑定人は必要に応じて記録を見ることもできる。鑑定人が遠方に住んでいたとしても、そこから質問に対して答えることができる。今、東京地裁では医療訴訟でカンファレンス鑑定ということをやっていて、複数の鑑定人に法廷に集まってもらっているが、これも一堂に集まってもらう必要はなくなるだろう。ウェブ会議を活用することによって鑑定人になる専門家の範囲を広げることもできる。例えば、日本全国の大学の中で何人かの鑑定人を選んでテレビ会議で、あるいはウェブ会議でカンファレンス鑑定をしてもらうということもできる。このような広がりが見込めるところに大きな期待があるのではないかと思う。

- 私もウェブ会議などの方式によって人証調べを行うという可能性、道を広げていくことについては賛成しているところで、問題はどのような場合にその方法をとるのかの判断を、誰がどのようなことを考慮して行うのかということかと思っている。その点については結局は裁判所の判断で行うべきかと思っているが、当事者の意見をどのように考慮していくのかというのは、今後検討が必要かと思う。
- 資料１の（５）で、ウェブ会議等による人証調べを行う場合に何らか支障が想定できるのではないかと指摘されているかと思う。具体的には当事者の尋問権や裁判所による訴訟指揮権の適切な行使が確保できるのかという問題意識かと思うが、少し想像してみると、証人なり尋問をする者がウェブでつながっているという状況を考えると、法廷で行われる場合の尋問と比べて、どうしても秩序の維持に難が生じやすいということは避けられないのかと思う。
- ここで指摘されている実務的検討や検証というのは、そのような問題をできる限り軽減していくための工夫を考えるということかと思っているが、これはゼロにすること

はそもそもできないものかと思うので、そのようなものであることを踏まえてウェブ会議で行うことが適切な事案なのかどうかを、裁判所が最終的に判断していくという設計にせざるを得ないのではないか、また、それはそれで構わないのではないかと考えている。

- （６）の公開の原則について、現在でも公開法廷で人証調べはしているわけだが、その場合に録画、録音等はできない。ある意味で公開と言っても限度のある公開をやっているということが言えると思う。これは証人をインターネットでさらし者にしないとか、その意味から非常に重要なことが行われていると思いう。また、今の憲法がつくられたときの公開と現在、インターネットで公開されているのとは全然違った意味でのレベルの公開になっていると思うので、このあたりはしっかり守ったままやっていく必要があるのではないかと思う。その意味では、これは（11）にも関係するが、例えばインターネットでその状況を録音、録画できるようなやり方をするのはまずいのではないかと思っていて、公開の方法や通信のセキュリティについても、十分な配慮が必要だと考えている。

- 人証調べのウェブ会議の活用について、刑事事件であったが、イギリスで裁判の傍聴に行った際に、被疑者を法廷に連れてくるコストをカットするために、拘置所でウェブ会議システムを裁判所とつないで、モニターに被疑者を出して人証調べが行われていたのを傍聴したことがある。傍聴した法廷は、e-Courtという点においてIT化が整った法廷ではなく、モニターもそれほど大きくはなかったが、スムーズに人証調べが行われていた。このような形でコストカットができるのであれば、遠隔地で居住しているという方の人証調べ等にウェブ会議を活用することができるのではないかと思う。
- アメリカでは、口頭弁論（Oral argument）の様子がYouTubeで見られる場合もある。あるいは社会的に影響の大きな事件になるとテレビで生中継されたりする。

- 公開の仕方について、当事者が勝手に録音をして公開するとか、期日に参加している会議室に公衆を入れて見せるとかいうことは想定されていなくて、当事者はクローズドなスペースで期日に参加して、傍聴は裁判所が設定したやり方で行うということで公開を実現するのがふさわしいのではないかと思う。
- あと、本人訴訟の場合に、法律事務所を使うというのも１つあり得る。自治体には既にLGWANという専用回線で実現された回線品質やセキュリティが確保された回線があるので、これをうまく使えば追加のコストをかけずに安全なe-Courtが実現できると思う。
- できれば自治体から既存のカメラ、マイクつきのパソコンを貸していただいて、自治体の会議室で、本人は参加することにすれば追加コストはかからないし、安全である。

さらに自治体の会議室なので、第三者が介入して見えないところから尋問の答え方を示唆することも防げる可能性が高い。

- （７）のITツールの活用という項目についても賛成で、ウェブ会議システムであれば文書表示機能がシステム上あると思うので、そのような機能も使って、遠隔地にいる証人に証拠の一部を提示することも可能かと思う。
- タブレットで手書きできる機能があれば証人が見取り図を描いたりして、それを調書に添付することも、システム上、保存するといったこともできるかもしれないし、既存の甲号証、乙号証で地図などに、「私はここのあたりにいた」ということをメモして、それをそのまま調書添付できるといったようなテクノロジーもあり得る。
- （８）書証取り調べについて、韓国での取り扱いでは原本確認はほとんどしなくなったという話を裁判官から聞いていて、当事者及び裁判所が原本確認の必要があると考えたものだけを出頭した期日において確認するという取り扱いになっているようだ。日本でも現実的には原本があるものでも写しで提出して、原本確認を省略するようなことが実際に行われたりしているので、その扱いをｅ裁判においてもうまく取り込んでいくような方法が望ましいのではないかと思う。
- （９）の送付嘱託・調査嘱託についても、e-filingの一環として当然デジタルで出してもらえれば出してもらう。ただ、これは協力いただくという側面があるので、紙で提出することも当然できて、その上で裁判所なり当事者なりがデジタル化することになるのかなと考える。
- （13）でIT化のプロセスということで、導入のハードルが比較的e-Courtのほうが低いのではないかということについても賛成で、e-filingの場合はどうしてもシステム構築が必要だが、e-Courtは当事者のハードウエアを活用できるという側面がある。また自治体のLGWANみたいなものも活用できることがあるので、規則改正等の必要はあると思うが、ハードウエア的にはe-Courtのほうがハードルが低いと思うので、実現においてはこういうことが考えられるのかなというところである。
- 最後の２の最終口頭弁論でのe-Court、e-Managementの問題なが、これもまさに記載のとおりである。特に人証調べの後は裁判所の心証も固まってきて、その開示等々によって和解の機運が高まってきているタイミングだと思うので、そのタイミングで、e-Courtを活用して機動的にどんどん期日を入れて、和解に近づけていくことが可能になると期待できる。
- それから、この段階では各種主張書面、証拠が出そろっているので、それを踏まえて最終準備書面を書くことになるが、その際に非常にたくさんの書面や証拠があると、紙を一生懸命めくりながら書いているわけだが、それが画面で簡単に閲覧しながら書けると便利である。それから、コピペもできるので引用も非常に簡単で、最終的な書面の取りまとめが非常に簡単になると思っている。

- 実は現行のやり方のテレビ会議でも、裁判所ごとにいろいろな運用の工夫があるそうで、先ほど委員が指摘になったカメラに映らない後ろから証人を操るというようなことがないように、必ず事務職員をつき添わせることにしている裁判所もあるように聞いている。そのため裁判所の協力、事務総局の協力も得て、各地の裁判所の実務上の運用ルールがどうなっているのか、いろいろ問題点とかも出していただくのも一案かなと思う。
- （８）の人証以外の証拠の取り調べについては、資料にあるように文書の性質や内容、成立の真正に関する争いという場合には、このようなデジタルなものの真正性などをまさにテレビ会議で口頭で言い合っていてもしようがないので、デジタルな性質に合わせたフォレンジック技術を使うとか、そのような証拠調べのあり方の検討が必要かと思う。

- 公開について、現在、法廷で録画、録音をすることは許されていない。その基本的な理由は裁判を劇化しないということが言われているが、インターネットで法廷の審理が流され、録音、録画されると審理内容が改変されてしまうおそれも生じる。AIを使ったフェイク動画がつくられるようになっているので、改ざんされてまた流布されるという新たな危険が生まれていると思う。そのようなことは止めなければならないだろう。
- 裁判所の方で法廷での尋問を録音し、それを文字化することはこれとは別で、これについては、法廷での証言は直ちにAIを使って文字化するという方法を取り入れていただきたい。当事者としては早く文字化したものが見たいということがあるだろうし、その利用価値は非常に高いだろうと思う。仮に本人は法廷にいないで今日法廷で何があったのか確認したいと思えば、その文字化された証言内容を直ちに見ることができる。
- 書証の取り調べは、既に写しで取り調べをするという実態があるので、成立に争いがある場合だけ原本を確認するということをやればいい。ウェブ会議でやることは現在と余り変わらないだろうと思う
- セキュリティレベルに関しては、現在、電話会議でも盗聴されている可能性があるわけだし、録音もされる可能性があるわけなので、テレビ会議やウェブ会議になるからといって、それを超えてそれほど高いセキュリティレベルを考える必要はないのではないかと思う。
- e-Courtは、利便性の高い技術なので、e-Courtについてはできるだけ早く実現して、より便利な裁判ができるようにしていただきたいと思っている。

- e-Courtで人証調べを行ったというときに、それをどのように訴訟の記録にしていくのかということについては検討が必要だと理解している。具体的には人証調べの状況は

映像で記録されることが可能であって、その記録された映像そのものを訴訟記録の一部にすることは大いに検討の余地があるのではないかと個人的には思う。ただ、例えば上訴された場合に、上訴審の裁判官がその人証調べの状況を効率的に把握する必要があるわけで、映像記録しかないという状態だと、現実問題としてはその記録を全て実際に見るというのはなかなかつらいものもあるのではないかと思うので、反訳というのはどうしても必要になってくると思う。

- 訴訟の当事者の観点からすると、反訳ができてきたときに、それが実際の口頭におけるやりとりを正しく反映しているのかということを逐語調書の場合にはチェックするわけだが、その意味でも映像で記録された人証調べの状況を訴訟の当事者が閲覧して、それが反訳と合致しているのかといった点を確認することができる仕組みをつくっていくことが有益ではないかと感じている。
- 資料１の（７）で人証調べにおけるITツールの活用について、ITツールを使うことによって、メリハリのついた効率的・効果的な尋問を行うということで、そのような検討をしていくということ自体はもちろん否定するものではない。この点についても先ほど説明したとおり、人証調べの結果が上訴審でも参照されることになると思うので、実際にその人証調べの場にいない裁判官であったとしても、その状況がわかるようなプラクティスをつくっていくことが必要だと思う。これはまさに実務運用の話でもあろうかと思うが、検討会においても一言申し上げたほうがよいと思う。

- 銀行は法人として、銀行自身が訴訟の当事者になる場合もあるし、あるいはお客様同士の争いの中で、従業員が証人として出廷する場合もある。このような場合、銀行としてはコストもさりながら、従業員、特にもともとの職場から遠隔地に異動済みの従業員が証人に呼ばれるようなケースにおいては、移動の時間とか、あるいは本人の負荷とか、そういった点を鑑みると、ぜひともウェブ会議による遠隔地での人証調べの拡大というのは、推進していただけると大変ありがたいと感じている。
- 実際に証人尋問のリハーサル的なことを当然ながらやるわけだが、その際、遠隔地の従業員などの場合は、社内のシステムとか、あるいは弁護士事務所のシステムを借りて、遠隔地のウェブを通じてリハーサルをすることもある。それが何かそれほどやりにくいことであるとか、実際にリアルに対面でやるときと大きく違いがあるのかというと、それほど違いはないのではないかという実感を持っている。
- あと、遠隔地という意味では先ほど海外という話が少し出たと思うが、これについてはやや慎重に考えたほうがいいかなと思っている。海外となると、そもそも現地の領事館なりそういうところというのは数が限られるわけで、例えば海外にいる従業員の場合、証人として海外の日本の領事館に行くぐらいだったら、いっそ東京に帰るよというケースもある。実際に東京に来てもらったほうが準備も、代理人の方との打ち合わせもできるし、我々の都合だけで何かお願いするつもりは全くないが、海外でもで

きるようになるという選択肢を設けることは構わないと思うが、例えば実際に人証調べをどこでどのようにやるか、裁判所による訴訟指揮に際して、そのようなところも配慮いただけると、実務的には大変助かるのではないかと思う。

- 公開について、国民性だとか国民の意識というものが大きく違うことは最低限、踏まえていただきたいと思う。例えば、海外では亡くなった方の顔を映像で公開しているようなケースがあるが、日本人としては違和感がある。こうしたことがまずベースにあると思う。
- 現状、公開されていると言えども、いつ、誰の裁判が、どこで行われるということがネットで公開されているという状況ではないと聞いているので、直接裁判所に行って調べて、今日は何があるということが分かるということだと思うし、傍聴するための手続というものも最低限必要なわけなので、そのようなレベルを維持するようなIT化ということを考えていただきたい。そうでないと裁判をすること自体を阻害するようなことになってはいけないと思う。
- もう一つは、例えば動画で流されるというようなことになると、炎上することもあって、裁判の判断に影響を与えるということはあると思う。最近、国の会議なども公開されている中で、それに対する意見というのがさまざまな形で寄せられるということがあるので、それが大きく広がるようなこともあるのではないかということ。
- もう一つ、ウェブ会議を実施する部屋とか環境などについては十分に御検討いただきたいということは、重ねてお願いしたい。

- 参考資料１で、一定の配慮が求められる訴訟記録についてという中に、非公開を前提とする弁論準備手続のやりとりを記載した調書という記載がある。現実にはほとんどの争点整理が弁論準備手続で行われているので、その意味ではこの手続は非常に重要であるが、これが非訟事件と同じような意味で非公開だという頭で物事を考えると、ちょっと問題があるかなと思っている。
- というのは弁論準備手続でやっていることは、本来、公開の法廷でもできる内容で、手続を公開しない旨の定めもない。そういう意味では手続を公開しない旨定められている非訟事件だとか家事審判手続の審理とは違う。弁論準備手続は、当事者が自由に発言しやすいようにということで公開を要しないことにしているだけで、中身は公開してもいい性質のものだということだけは、注意しておかなければいけないと思っている。

- 先ほど、どの範囲で、どのような内容が、一般の人々の目にさらされることとして受け入れられるのかという話もあったかと思う。本日の会議の前半ではセキュリティについての説明もあったが、そのセキュリティの対策によって何を守るのかということ

については、裁判手続のIT化の上では少し検討を深めて整理をする必要があるのではないかと思う。

- 一般には営業秘密だとか、個人の私生活上の重要な秘密というもの、これが保護の対象になるということは異論はないのかと思うが、IT技術によって一般の人が誰でもいろいろなことを知ることができるという環境のもとでは、例えば個人が訴訟の当事者になっているという事実そのものとか、あるいは人証調べの場において非常にしどろもどろした発言をしているという映像が人々の目にさらされるということ、こういったこともセキュリティによって守るべき対象として考えるべきなのではないかという気もしている。
- そのような裁判手続に特有の問題というのが、これまで一般に考えられているセキュリティ対策の議論の中で十分にすくい取れるものになっているのかどうかということについてはやや疑問を持っているので、何が守られるべきなのかということについては細やかな議論をする必要があるのではないかと思う。

- 先ほどウェブ会議等による人証調べの期日の公開のあり方についての意見があったが、確かに日本の国民性は他の諸外国と異なる点があるので、その点はもちろん考慮しなければならないが、諸外国とは異なり、現在、日本では裁判期日をホームページ等で公開しているわけではないので、その日にどのような裁判が行われるのかということは、実際に裁判所に行かないとわからない。したがって、今後、ITツールを活用した認証調べ等が普及した場合に、実際に裁判所に行ったものの、その日の裁判が全部ウェブ会議等で行われてしまっていて、傍聴ができる裁判がほとんどないというような事態が生じることも考えられなくもないので、そうなると期日をどこまで公開するのかというのは、公開原則との関係からも慎重に考えなければいけないのだろうと思う。
- 参考資料１の訴訟記録のこれはセキュリティとの関係について、ここで注意しておかなければいけないのは、「一定の配慮が求められ得る訴訟記録について」という点であると考える。この「一定の配慮が求められる」のは誰に対してかというと、一般公開をするという段階での配慮だと認識している。なぜならば、当事者等に対しては、訴訟記録に関する配慮というのは自分のことに関しての個人情報なので、そこに関しては配慮する必要はない。仮に訴訟記録が電子化されて、それを一般公開するかどうかという場合に配慮をしなければいけない範囲、すなわち第三者によって改ざん等ができないようにしなければならないといったことが求められると思うが、恐らく現時点では、電子化した訴訟記録を一般公開するかどうかという話は、まだそこまで詳細に議論されていないと認識している。事件の当事者、利害関係人等、特に当事者間において、電子化された訴訟記録をどのように共有するかという問題は、この「配慮を求め得る」訴訟記録をどのように保護するかという問題とはまた異なった問題であり、後者が一般公開をする段階での配慮とセキュリティレベルの話ということになる。そ

こは区別して議論をする必要があると考える。

- 公開の問題については議論が錯綜しているところがあって、民事訴訟制度としてどこまで公開を許容するのかを現代的なツールとの関係で議論していくという問題と、セキュリティの問題としてリスクがどこまであるからどう守るかという問題は別なので、民事訴訟制度をこう変えましょうという議論とセキュリティの議論を分けたほうがいいと思う。

- 山本座長
  もちろんこの公開の問題は、憲法で動かせない要件の部分もあるし、具体的な制度あるいは運用をつくっていく上においては、かなり慎重に対応していかなければいけない部分だと思う。

- 資料３の（２）にかかわるところについて、御意見を申し上げたい。ここでは判決のあり方についても、IT化を通じた争点整理手続に対応したものを検討することが期待されるのではないかという指摘がある。私としても争点整理のあり方を考えた上で、その最終成果物のことを念頭に置いた判決のあり方を検討すること自体には反対をするものではない。
- ただ、１点気になっているのは、判決が出ると場合によっては上訴審で検討対象となる。また、類似事件においてどういった判決が出るのかということを調査するときの資料にもなるという、そういう機能、意義もある。そうすると判決は一定のフォーマットに沿った形でつくられていないと、上訴審や類似事件を取り扱う者にとっては理解することが困難になる可能性があるのではないか。
- 一方、争点整理は、裁判所と訴訟当事者の創意工夫によってさまざまなバリエーションのあり方があると思うので、その争点整理の結果を判決に利用するときのやり方によっては、判決の姿というのがフォーマットとしてばらばらになってしまうこともあり得るのではないかと思う。そうすると先ほど申し上げた判決の持っている機能、役割の一部分が毀損することもあり得るように思われるので、その観点から注意をしながら判決のあり方を検討することが必要だと思う。
- もう一点、資料の３（４）について。ここでは判決の言い渡し期日のあり方について検討することが示されている。私自身も判決の言い渡し期日が少々形式的なものになっていることは否めないと考えている。裁判官の方が判決言い渡しにおいて、判決の主文を何件もまとめて連続して法廷で口頭で説明される。でも法廷にはほとんど誰もいないという、やや空疎な感じもするセレモニーのような面もどうしても存在する。
- これはIT化による解決の問題とは少し違うのかもしれないが、本当に裁判官が実際に口で判決を言い渡すことまでが憲法上の要請なのだろうかということも、個人的には

少し疑問を感じているところ。憲法で言っているところの公開とはどういう意味なのか、法廷とはどういう意味なのかということについては、現代の環境のもとで見直しをする、再考してみることは必要なのではないかと考えている。

- 判決だが、裁判官は本人訴訟も含めた千差万別の準備書面を読んでおり、中には手書きのものもある。これに対して判決は、基本的に一定の様式に従っているので、書き方がさまざまであるからといって戸惑うようなことはない。
- むしろITを通じた争点整理の結果が判決に生かされるということが大事だと思っている。争点整理表をITを使って両当事者と裁判官が協力しながらつくっていく、時系列表も同じようにしてつくっていく。そして、それを判決に使って判断をするということが争点に対して的確に答えることになるし、判決作成を迅速化することにもなるので、そのような審理を進める意味でこのIT化は大事だと思っている。
- 判決の言い渡しに関しては、世間の耳目を浴びるような事件は多くの傍聴人が来る、あるいは報道機関も来るが、そうではない事件に関しては当事者が来る事件もあるし来ない事件もある。誰も来ない事件も多いという状態。仮にテレビ会議やウェブ会議で立ち会えるようにしたからといって、立ち会う人が増えるかといったら増えないのではないかと思っている。むしろ早く判決の結果を当事者に届けることが大事ではないか。そういう意味では電子データで判決を作成して、言い渡したら直ちにそれが当事者のところに届くという仕組みができれば一番いいのではないか。
- 判決をアップロードして、アップロードしたということを当事者に伝えるというやり方が一番考えられるわけだが、判決の送達はとても重要なので、その確実性を担保する仕組みをつくっていかなければいけないだろう。

- まず５ページの（８）について、執行の手続のときに判決正本を現在は提出しなければならないわけだが、こういったことというのは今後、判決が電子化された場合には、裁判所相互の電子的な情報のやりとりでもかえられるようになるのではないかと考えている。こういったことは実は判決だけではなくて、いろいろな裁判関係の情報共有をどのように裁判所間で行っていくかという大きな枠組みの一環として考えていくべきだと思っている。
- これと少し関連して、４ページの（３）判決情報を電子情報で行うときにどう考えるかということだが、少し私としての考え方を紹介したい。この判決情報がどのように使われるかによって、このセキュリティレベルというのは相当変わってくるのではないかと思っている。仮に裁判所間でやりとりするので十分であれば、余り原本を改ざんするとかいうのは大きな問題が起こらない可能性が高いと思う。一応、理屈としては裁判所が後から書きかえたのではないかとか、そういう問題はなくはないけれども、そこまで考えるべきかということは出てくる。

- それ以外の場面として、民民で、民間同士でこういう判決が出たのだからというのを他人に示すような場合というのは、原本性というのはかなりしっかりやっておく必要があろうかと思う。
- 行政機関がこれを受け取るような場合というのは、これはどういうふうに行政機関と裁判所との間で情報共有していけるかという問題とも絡んでくるので、どういう場面で、どういうふうに使われるかということを踏まえて、リスクがどこにあって、どのように対応するかという観点から、ここはしっかり検討していく必要があるのではないか。

- 裁判をしてきた最終場面なので、送達を受け取れるかどうかというのはかなり本人の責任が大きいことは了解しているが、それでもなおパソコンの状況であるとか、突発的な状況というのがあるので、そこら辺も御検討いただきたい。
- それとは別に私どもの相談の中では、裁判が終わってから、それでもなお相談いただくケースが少なくない。要は裁判の判決をもらうことの意味合いであるとか、その後の手続をどうすればよかったとか、そういうことの理解が不足しているケースがあるので、せっかくIT化ということであれば、この期間に何をしなくてはいけないのであるとか、いつまでとか、そのような情報提供をともにしていただくことがある意味、メリットがあるのではないかと思う。

- まずセキュリティの（３）について整理すると、判決は公開法廷で言い渡されることを前提としているので、守秘性という観点、CIAのＣという観点では求められているセキュリティレベルはそんなに高くない。一方、権利義務の源泉となる書類なので、それを民民で渡し合うような事態が考えられるとするならば、改ざんは絶対にされてはいけない。ゼロを１桁多くして裁判所に持っていくと、それで執行が可能となってお金を詐取できるような状況は絶対に避けないといけない。つまり、完全性といった側面は非常に重要なものがあるだろう。
- （８）の他の手続との関係という点で言うと、これもどんどん情報共有を図っていければいいというのは大賛成。例えば、法務局への嘱託登記も今は紙で行っているが、それも行政連携で情報をつなげば、データで全部送れるということがあると思う。
- 民事執行では、配当手続とか、競売手続ということで、いろいろな当事者以外の関係人がかかわる手続なので、定型化しやすい。配当に関する計算式がシステムに入っていたりとか定型化しやすく、情報システムにとてもなじむ手続だと思うので、できるだけ自動化できるものは自動化していくのにはふさわしい分野なのではないか。もちろん通常訴訟を最初にやるというのが前提ではあるが、第２段階、第３段階で執行もやっていけばいいのかと思う。
- 最後に、判決原本をデジタル化することによって検索の容易性とか、引用の容易性と

か、そういった利便性が高まるので、他の手続や上級審等々で活用が容易になる。それを可能にするために判決文をどう扱っていくかという問題があるが、我々弁護士は、ふだん仕事をしていく上で、先例となる裁判例、判例を参照している。企業においても、これからどういうビジネスを展開するかというときには法律、判例、行政庁の通達といったものを総合的に考慮して行動する。そういう意味で判例というのは日本国民なり企業なりの予測可能性の源泉でもあると思うので、判決がデジタルになっているのであれば、それをできる限り広く公開するというのもIT化の範疇の１つに入ってくると思う。

- 現状、裁判所内の手続を踏んで公開すべき判決を決めていると思うが、残念ながらそんなに多くの判決が公開されているとは思えない状況がある。一方、第２回検討会の参考資料にある弁護士白書に掲載されている弁護士のニーズを見ると、約80％近い弁護士がより多数の判決の公開を望んでいるという実情もあるので、司法IT化の中で判決の公開も取り組むべき課題として入れていただければいいと思う。研究者の方も、たくさん公開されている判決がある方が研究が進むということもあると思う。

- ３（６）の判決書の送達について、（６）は恐らく控訴期間の話との関係で書かれているところだと思うが、これを確実に担保する必要があるというのはそのとおりだと思う。２週間なので、特に本人訴訟の当事者などは判決が届くこと、そして、それを受けた日から一定の期間しか控訴できないことをきちんと認識されているかも大事になると思うので、どこからそれが始まるのかという控訴期間の起算日になる日を確実にするためにも、きちんと判決が届く、送達されるということを確実にする必要があると考える。

- 先ほどから、ウェブ上で判決も含めて公開をすることへの懸念が各委員から指摘されているが、例えば動画像の中に電子透かしを埋め込むとか、いわゆるDRM（Digital Rights Management）と呼ばれている技術とか、技術的にはやろうと思えば幾つか方法はある。ただ現時点でも、傍聴人全員に厳格な所持品検査をして徹底して何も持ち込ませないというようなことまではやっていないが、電子化した場合に、どこまでやるか。そのようなリアルな法廷での盗撮の防止と電子化した場合を比較しながら、やろうと思えば技術的にはいろいろ方法はあると考えている。
- あと、判決だが、e-Govに載っている法令提供サイトのXML化をしたところ。せっかく電子化されているテキストなので、後での可用性を高めるという意味では、新しいやり方で公開を始めるテキストについては何らかの構造化をするというのも１つの考え方であると思う。これは別にさほど技術的にすごい手間がかかって大変ということでもないと思うので、この際、検討に値するのではないか。

- XML化については、私が聞いたところによると日本の商用データベースを販売している会社の中の一部は、既に判例に独自にXMLタグをつけて管理をしているとのこと。裁判所がつけてくれると願ったりかなったりだということはあると思う。

- 山本座長
  これでひと通り３段階に分けた手続の流れの議論については御議論をいただいたことになるので、今後はいよいよ取りまとめに向けた議論に向かう。
- 段取りとしては、あと２回のうち、次回はこれまで議論の中で通奏低音のように流れていた問題として、本人訴訟、特にITに十分な親しみがないような方々に対して、どのような対応を考えるか、これまでも議論はしてきていただいたところではあるが、一度まとめて議論をいただきたいと思う。それを踏まえて最終的なとりまとめ案を次回、次々回で議論をいただく。そのような手順を考えているが、その手順について何か意見があれば。

- これからこの検討会の取りまとめに進むということで、この検討会の作業の終わりも見えてきていると思うが、IT化自体については当然その後に話が続いていくことになり、どういった組織、どういった方々が何をしていくのかということは重要なものと考えている。
- その観点からいうと、IT化は中核的には裁判所におけるITシステムの構築というところが大きいと思っている。最高裁においてどういう対応を考えているのかということに関心を強く持っているところ。これは取りまとめの方向性にもかかわりが当然あると思う。最高裁にはこの検討会にオブザーバーとして参加いただいているし、第１回検討会ではプレゼンテーションもしていただいたが、何度か繰り返されてきたこの検討会での議論を踏まえて、現在、最高裁としてはIT化に今後どのように取り組んでいくことを考えているのか、現時点の考えをお話しいただきたいと思う。次回あたりにでもお話しいただけるとありがたい。
- ２点目だが、今後どのような制度検討をしていくのか、検討会の中では実務的な話もかなり多く出てきていたかと思う。そのような民事訴訟のプラクティスにかかわる部分は検討会の方向性を踏まえてのことになるが、法曹実務家が検討を続けていく。それは理論面もそうだし、実務面においてもそうだが、そうした検討を続けていくことが必須だと思う。いろいろな検討すべき論点とか実務的課題というのは、幾つかこの検討会でも言及されたと思う。
- ３月に検討会が終わった後に４月以降だが、そうした検討を引き継ぐべき法曹三者の検討の場というか、受け皿というか、そのような枠組みをどのようにすることになるのか。この点について法務省にはしっかりとした枠組みの検討をしていただきたいと思う。次回か次々回までには考えを聞かせていただきたいと思う。

- 山本座長
  今２つの意見をいただいた。これは最高裁と法務省それぞれにということだったかと思うが、現段階で話せることがあれば伺いたい。

- 藤田参事官（法務省大臣官房司法法制部）
  我々としてもここで御議論いただいた方向を今後、しっかり受けとめる実務的検討が不可欠だろうと思っている。裁判のIT化は、司法、裁判所にかかわる問題なので、司法権の独立への十分な配慮は不可欠と思うが、法務省として、司法制度を所管する立場から、４月以降どのような形でこの議論を受けとめるかについては、この検討会の場で報告できるように検討、準備を進めたい。

- 成田課長（最高裁判所事務総局民事局）
  この検討会を踏まえて当然内部でも検討している。現時点で次回説明するとは確約しにくいが、委員からの指摘も踏まえて、できる限りそのような場を設けられるように準備をさせていただきたい。

- 山本座長
  ありがとうございます。座長としてもぜひ御尽力いただきたいと考えている。

（以上）