

第 1 1 回検討会資料

第 1 認証紛争解決手続の期日がウェブ会議等で実施される場合において、同手続において示された秘密を適切に保持するための取扱いについて

1 前回の検討会における議論

- (1) 多くの認証紛争解決事業者においては、認証紛争解決手続の期日をウェブ会議等で実施することが喫緊の課題となっていることを踏まえ、前回の検討会においては、認証紛争解決手続の期日がウェブ会議等で実施される場合の秘密の取扱いの問題に焦点を当て、ウェブ会議等で開示された秘密保持の在り方のほか、これに関する実施ガイドラインの改正の可否、法第 1 2 条第 1 項に基づく変更認証の可否等について議論が行われた。
- (2) 前回の検討会においては、期日が対面で実施される場合と比較して、ウェブ会議等で実施される場合に高まる秘密保持上のリスクとして、事務局から以下の 1 ①ないし④のリスクを提示し、これに基づき議論が行われた（別表参照）。

1 認証紛争解決手続をウェブ会議等の方法により実施する場合の秘密保持上のリスク

- ① 第三者が（インターネット上で）ウェブ会議等を覗き見るリスク
- ② 当事者が録音・録画等を行うリスク
- ③ 第三者が（物理的に PC 画面を見る等して）ウェブ会議等を覗き見るリスク
- ④ ウェブカメラの死角等から、代理人でない第三者が当事者に指示等を行うリスク

2 法第 6 条第 1 1 号及び第 1 4 号に係る実施ガイドラインの見直しの可否について

○ 法第 6 条第 1 1 号に係る現行ガイドライン

法第 6 条第 1 1 号の「これを適切に保持するための取扱いの方法」とは、当該方法によれば秘密が適切に保持される蓋然性が客観的に認められる具体的な方法をいう。

例えば、秘密が記載されている文書等の管理に関する規程類の整備、管理責任者の設置、当該文書等の盗難防止策、当該文書等へのアクセス制御等、秘密の安全管理のための組織的、物理的、技術的な措置を講じていることは、これに該当する。

○ 法第 6 条第 1 4 号に係る現行ガイドライン

法第 6 条第 1 4 号の「秘密を確実に保持するための措置」とは、当該措置を実施すれば秘密が確実に保持されることの蓋然性が客観的に認められる具体的な措置をいい、例えば、秘密保持契約の締結、秘密が記載されている文書等の管理に関する規程類の整備、管理責任者の設置、当該文書等の盗難防止策、当該文書等へのアクセス制御等、秘密の安全管理のための組織的、物理的、技術的な措置を講じていることは、これに該当する。

- (1) 前回の検討会における議論

ア 前回の検討会においては、法第6条第11号及び第14号に係る実施ガイドラインには、期日がウェブ会議等で実施される場合の秘密保持に関する具体的な基準等を記載すべきではないとの意見が大勢を占めた。

その理由として、情報通信技術等は日進月歩であるため、実施ガイドライン上にあるべきセキュリティ対策等の内容が具体的に記載されたとしても、その後の技術の進展等により、記載が陳腐化してガイドラインとしての実効性を欠くものとなるおそれがありはしないか、他方で、そのような事態とならないようガイドラインの常時見直しを図るとしても、煩瑣であるだけでなく、ガイドラインとしての安定性を欠き、これまた実効性を欠くこととなりはしないかとの不都合を指摘するものや、どのようなセキュリティ対策等を講じるかは、認証紛争解決事業者のポリシーによるべき性質のものもあると指摘するものが見られた。

また、前回の事務局資料においても、手続の非公開性は、手続で示された秘密を保持するための一つの方策にすぎず、それ自体が認証基準として求められているわけではない上、手続の非公開性は、様々な規律をもうけ、措置を講ずるなどして、総合的に非公開の実質が損なわれないような仕組みを構築することで実現していくものであり、殊更にその一部のみを取り上げて、実施ガイドラインに具体的に記載することの妥当性についても指摘していたところである。

イ 一方、法第6条第11号及び第14号に係る実施ガイドライン上に、期日がウェブ会議等で実施される場合の秘密保持に関する具体的な基準等を記載すべきではないとしても、抽象的な文言であれ、セキュリティ対策を講ずるべきことを記載することが考えられるのではないかとの意見も出された。このような意見に対しては、現行ガイドラインの「秘密の安全管理のための組織的、物理的、技術的な措置を講じていること」に包含されていると解されるとの意見も出された。

(2) 検討の方向性

期日がウェブ会議等で実施される場合の秘密保持の在り方については、ウェブ会議特有のセキュリティ上の問題点も含め、秘密漏えいのための方策を講ずる必要性があることで大方の意見の一致を見たものの、法第6条第11号及び第14号に係る実施ガイドラインを見直すべきか否かについては、意見が分かれた。これまでの急速かつ広範な情報通信技術の進展状況等に照らせば、実施ガイドライン上に講ずるべきセキュリティ対策の具体的基準等を記載することは、ガイドラインの実効性確保の観点からは問題があり、他方で、実施ガイドライン上にセキュリティ対策の構築が各号の基準適合性審査において重要な考慮要素となることを追記することも十分に考えられる。もっとも、現時点においては、期日がウェブ会議等で実施される場合における秘密保持の在り方に限局して検討が行われたものであり、今後、ODRにおけるセキュリティ全般について検討が行われることが予定されている。以上を踏まえ、現段階においては、法第6条第11号及び第14号に係る実施ガイドラインの見

直しは行わないこととし、ODRにおけるセキュリティ全般について検討が行われる際に、改めてガイドラインの見直しの要否等について検討することでどうか。

3 法第12条第1項に係る実施ガイドラインの見直しについて

○ 法第12条第1項に係る現行ガイドライン

7(1) 変更の認証について（法第12条関係）

変更の認証を要しない軽微な変更のうち、規則第10条第3号の「認証紛争解決手続の業務を行う知識又は能力の減少を伴わず、かつ、紛争の当事者に負担の増加その他の不利益を及ぼすことがないもの」については、例えば、次の変更がこれに該当する。

ア～ソ （略）

(1) 前回の検討会における議論について

ア 前回の検討会の事務局資料においては、期日の実施方法を変更して、対面による手続に加えて、ウェブ会議等を追加する場合において、期日の実施方法につき対面による手続とウェブ会議等による手続とを当事者が選択できるものであれば、秘密が漏えいするリスクについて、対面による手続とは異なった観点からの検討を要し、その対応如何では、当事者に不利益が生じるおそれがある点を除けば、規則第10条第3号の「証紛争解決手続の業務を行う知識又は能力の減少を伴わず、かつ、紛争の当事者に負担の増加その他の不利益を及ぼすことがないもの」に該当すると考えることもできるとの考え方を示した。

イ この点について、前回の検討会においては、対面による手続にするか、ウェブ会議等による手続にするか、当事者が選択できる形で導入するのであれば、必ずしも変更の認証を要するものとする必要はなく、変更の届出で足りる場合を認めるべきであるという意見が出され、これに反対する意見は見られなかった。もっとも、秘密漏えいのリスクとの関係で、具体的にどのような場合に変更の届出で足りるとすべきかについては、今回の検討会で続行して議論することとされた。

ウ 仮にアの考え方を採用しつつ、イの意見にあるように一定の場合には変更の届出で足りるものと整理することができるとしても、法第12条第1項ただし書の「軽微な変更」の該当性については、認証紛争解決手続の業務としての適格性が維持されているかどうかについての再審査を不要とすべき例外的事情があるかという観点から判断されるべきものであることからすると、変更後の期日の実施方法については、秘密保持の観点からも当事者に負担の増加その他の不利益を及ぼすことがないものであることが、変更後の規程類や措置により外形的に明らかであることが必要であると考えられる。また、その判断は、第一次的には、業務の実施方法を変更しようとする認証紛争解決事業者においてされるべきものであることからすると、この点に関する実施ガイドラインの見直しをするのであれば、

認証紛争解決事業者において変更の認証の要否について容易に判断することができる記載振りとする必要があると考えられる。

以上を踏まえ、期日がウェブ会議等で実施される場合に想定される①から④までの秘密漏えいのリスクについて、どのような規程類を整備し、措置を講じていれば、秘密保持の観点から当事者に負担の増加その他の不利益を及ぼすことがないものであることが外形的に明らかであるとして変更の認証が不要とされるのか、また、そのことを実施ガイドラインにどのように表現すべきか、以下、若干の検討を加えることとする。

(2) ①のリスクについて

ア ①は、期日がウェブ会議等で実施される場合において、第三者が不正アクセス等を行うことで、期日でのやり取りを覗き見ることによる秘密漏えいのリスクである。この点、本検討会で実施されたヒアリングでは、Microsoft Teams等の現行の汎用的なウェブ会議システムにおいては、最新版にアップデートされたものが使用されるのであれば、通信の暗号化措置が施されているため、第三者による盗聴等がされることは技術的には考えにくいとのことであった。したがって、通信の暗号化措置が施されたウェブ会議システムを使用する旨の規律が設けられ、そのような措置が講じられているのであれば、秘密保持の観点から当事者に不利益を及ぼすことがないものであることが外形的に明らかといえる。

イ コンピューターウイルス感染を原因とするウェブ会議等の内容の漏えいのリスクについては、認証紛争解決事業者（手続実施者を含む。）及び当事者において、一般的なセキュリティ対策（例えば、セキュリティソフトを導入したり、OSを最新版にアップデートしたりする等）が施された端末を使用することで基本的に対応することができると考えられ、そのような環境でウェブ会議等が実施されるのであれば、秘密保持の観点から当事者に不利益を及ぼすことがないといえる。したがって、認証紛争解決事業者（手続実施者を含む。）及び当事者において、一般的なセキュリティ対策が施された端末を使用することを義務付ける旨の規律を設けることが必要でないかと考えられる。

もっとも、上記のような規律を設け、規程類を整備したとしても、当事者がその規律に違反して、セキュリティ対策の不十分な端末でウェブ会議等に参加する可能性は否定できない。そのような観点からは、当事者に不利益を及ぼすことがないものであることが外形的に明らかであるというには、上記のような規律を設けるだけでなく、その規律の実効性を確保するため、認証紛争解決事業者において、当事者の使用端末のセキュリティ対策の有無や内容の確認を求める旨の規律まで設ける必要があるか、なお検討を要する。この点、認証紛争解決事業者において、当事者の使用端末のセキュリティ対策の有無や内容を客観的に確認することは困難であるといわざるを得ない。また、当事者から使用端末のセキュリティ

対策の有無や内容を事前に申告させて、所定の要件を満たしている場合にウェブ会議による参加を許可するような規律を設けることは考えられる。しかし、結局は当事者の自己申告にすぎないため、上記のような規律を重ねて設けることによる効果も限定的なものと考えられる（もとより、そのような運用によることが望ましいことはいうまでもない）。また、現在幅広く活用されているウェブ会議においても、一般的には、参加者に使用端末のセキュリティ対策について事前申告させるような取扱いはされておらず、そのことがセキュリティ対策の観点から特段問題視されている状況にあるとはいえないように思われる。また、上記規律を設けた場合には、ウェブ会議等を実施する前の確認手続が煩雑となり、ウェブ会議等の利便性が失われることも懸念されないではない。

したがって、認証紛争解決事業者（手続実施者を含む。）及び当事者において、一般的なセキュリティ対策が施された端末を使用することを義務付ける旨の規律を設けることは必要であると考えられるが、それ以上に、認証紛争解決事業者に当事者の使用端末のセキュリティ対策の有無や内容について確認する旨の規律を設けなくとも、秘密保持の観点から当事者に不利益を及ぼすことがないものであることが外形的に明らかと評価できるのではないか。

ウ 以上からすれば、ガイドラインにおいては、届出で足りるとするための①のリスクの対応策の一例として、認証紛争解決事業者（手続実施者を含む。）及び当事者が、一般的なセキュリティ対策がなされた端末を使用し、認証紛争解決事業者（手続実施者を含む。）が、通信の暗号化措置が施されたウェブ会議システムを使用することを条件として記載をすることが考えられるかどうか。

(3) ②のリスクについて

ア 非公開とされたウェブ会議等でのやり取りを録音・録画した上、そのデータを放送、公衆送信すること（例えば、インターネット上にアップロードする等）は、非公開の実質が損なわれ、期日でのやり取りに含まれる秘密を著しく害するものであるから、秘密保持の観点からこれを禁ずる旨の規律を設けることが相当であると考えられる¹。

イ もっとも、当事者による録音・録画については、そのデータが流出するリスクが高まるという面があるが、それによって直ちに秘密の漏えいが生ずるものではない。この点について、前回の検討会においては、期日でのやり取りの内容を備忘のために録音・録画したいとの当事者のニーズも考えられ、そのような場合も含めて一律に禁止することは妥当ではなく、その可否等については、認証紛争解決事業者の自主性に委ねてよいのではないかと意見が出された。

もっとも、民間紛争解決手続の特性の一つは、それが非公開で行われることにあ

¹ 手続の非公開を前提とする場合の帰結であって、手続の非公開を前提としないのであれば、この限りではない。

り、それより、紛争の当事者は、安んじて秘密に属する事項を率直に明らかにし、それ故に、真実が明らかになり、あるいは紛争の実体に迫ることによって紛争の解決に至る蓋然性も高められることが期待されている（第9回検討資料の別紙1(2)イ）。また、認証紛争解決手続を利用する当事者は、一般的には、相手方当事者による録音・録画がされてないことを想定して期日に臨んでいるものと考えられる。前回の検討会においても、委員から、仮に当事者による録音・録画を許すのであれば、その旨を当事者に告知すべきである旨の意見が出されたところである。以上からすれば、認証紛争解決事業者としては、一般的には、当事者に対して、録音・録画の可否について説明することが適当であると考えられる。

なお、当事者による録音・録画を認めないこととする認証紛争解決事業者又は手続実施者において、当事者による録音・録画等がされていないことを確認することは困難と思われる上、対面による手続においても、録音・録画等のリスクはあるものの、所持品検査等の厳密な確認まで実施している認証紛争解決事業者はほとんどいないと考えられること等を考慮すると、認証紛争解決事業者又は手続実施者に、録音・録画を認めない旨を説明することに加えて、録音・録画のおそれがないことの確認義務まで要求することは均衡を失うと考えられる。

したがって、録音・録画の可否のほか、そのことを当事者に対して事前に説明する旨の規律を設けるとともに、放送・公衆送信を禁ずる旨の規律を設けることにより、秘密保持の観点から当事者に負担の増加その他の不利益を及ぼすことがないものであることが外形的に明らかであると考えられるのではないかと。

ウ 以上からすれば、②のリスクに対応するガイドラインにおいては、一例として、**録音・録画の可否について当事者に事前に説明するとともに、放送・公衆送信を禁ずることを条件として記載をすることが考えられるかどうか。**

(4) ③、④のリスクについて

ア 従来に対面による手続においても、非公開で実施するものとされた期日について、第三者がやり取りを容易に聞き取ることができる場所で実施したり、特段の規律を設けることなく第三者同席の下で実施したりすることは、一般的には、期日で示された秘密を保持するための取扱いを定め又は措置を講じているとはいえないものと考えられる。そのこととの比較からすれば、期日がウェブ会議等で実施される場合においても、手続実施者又は当事者が、第三者がやり取りを容易に聞き取ることができる場所でウェブ会議等に参加することや、第三者がウェブ会議等を視聴することがないようにすべきと考えられる。したがって、秘密保持の観点から当事者に不利益を及ぼすことがないものであることが外形上明らかというには、第三者がウェブ会議等を視聴できない環境で参加することを手続実施者及び当事者に義務付ける旨の規律を設けることが必要になると考えられる。

イ 一方、上記のような規律を設けることだけで、秘密保持の観点から当事者に不利

益を及ぼすことがないものであることが外形的に明らかといえるかについては、別途検討する必要がある。

この点、第三者がやり取りを容易に聞き取ることができる場所でウェブ会議等に参加することを防ぐ対策を徹底するためには、上記のような規律に加えて、当事者がウェブ会議等に参加する場所を自宅に限ることとしたり、又は事前に参加場所を届け出ることを要することとしたりする旨の規律を設けることも考えられる。しかし、現状のビジネス等の場面におけるウェブ会議等の運用においては、そこまでの対応を求めることが一般的になっているとは言い難く、セキュリティの観点からそのことが特段問題視されている状況にはないように思われる。現に期日をウェブ会議で実施している弁護士会に対するアンケート結果（第8回検討会資料3）においても、そのような規律を設けている弁護士会は存在しないとのことであった。

また、第三者がウェブ会議等を視聴するおそれがあるとの懸念については、当事者の関与なくしてこのような事態が生ずることは考え難いのであるから、当事者の申告によって防止することは困難であるといえる。この点について、第8回検討会の事務局作成資料においては、手続実施者が期日の開始前に、当事者にウェブカメラで室内を映してもらうなどの方法により、第三者が存在していないことを確認することをその対策の一例として示したところであるが、委員からはそのような対策までの必要はないのではないかと意見が出された。また、現状のビジネス等の場面におけるウェブ会議の運用においても、そのような対応を求めることが一般的とはいえず、セキュリティの観点からそのことが特段問題視されている状況にはないように思われる。そればかりか、現状は、バーチャル背景機能や背景のぼかし機能を活用して、実際の背景が映らないようにしてウェブ会議に参加することが一般的なものとなりつつある²。特に、自室からウェブ会議に参加する当事者からすれば、自室の隅々までウェブカメラで映して手続実施者や相手方当事者に示すことに心理的抵抗感を持つことも容易に想定できるところである。また、仮に手続の冒頭に第三者が同席していないことをウェブカメラの映像で確認したとしても、手続の途中から第三者が関与する可能性までを排除できるものではない。

以上からすると、第三者がウェブ会議等を視聴できない環境で参加することを手続実施者及び当事者に義務付ける旨の規律を設けることで、当事者に不利益を及ぼすことがないものであることが外形的に明らかといえ、それ以上の対策までは必要ないのではないかと考えられる。

² 本検討会で実施したヒアリングにおいては、ウェブ会議の背景から機密情報等が漏洩するリスクも指摘されていたところであり、その観点からは、背景等は映さない方がセキュリティ対策として優れているともいえる。

ウ 以上からすれば、③、④のリスクに対応するガイドラインにおいては、一例として、第三者がウェブ会議等を視聴できない環境で参加することを手続実施者及び当事者に義務付けることを条件として記載をすることが考えられるかどうか。

(5) 新ガイドラインの試案

以上の検討結果を踏まえた上で、前記(1)ウのガイドラインの明確性の観点をも考慮し、以下のようなガイドライン案を置くことについて、どのように考えるか。

○ 第12条第1項のガイドラインの試案

7(1) 変更の認証について（法第12条関係）

変更の認証を要しない軽微な変更のうち、規則第10条第3号の「認証紛争解決手続の業務を行う知識又は能力の減少を伴わず、かつ、紛争の当事者に負担の増加その他の不利益を及ぼすことがないもの」については、例えば、次の変更がこれに該当する。

ア～コ （略）

サ 例えば、①認証紛争解決事業者(手続実施者を含む。)及び当事者が、一般的なセキュリティ対策がなされた端末を使用すること(例えば、使用端末にセキュリティソフトを導入する又はOSを最新のバージョンにアップデートすることは、これに該当する。)、及び認証紛争解決事業者(手続実施者を含む。)が、通信の暗号化措置が施されたウェブ会議システム(最新のバージョンにアップデートされた一般的に使用されているウェブ会議システムは、これに該当する。)を使用すること、②認証紛争解決事業者(手続実施者を含む。)が、録音・録画の可否を当事者に事前に説明するとともに、録音・録画を認める場合には、放送・公衆送信を禁ずること、③許諾を得ていない第三者がウェブ会議及びテレビ会議(以下併せて「ウェブ会議等」という。)を視聴できない環境で参加することを手続実施者及び当事者に義務付けること等のウェブ会議等における秘密を保持するための取扱い及び措置を定めた上で、対面による期日の方法に加えて、ウェブ会議等による期日の方法を追加する変更(ただし、当事者が、自身が対面により期日に参加するか、ウェブ会議等により期日に参加するかを選択できる場合に限る。)(法第6条第11号、第14号関係)

シ～タ （略）

4 ガイドライン改正以外の方法による情報提供について

前回の検討会においては、具体的なセキュリティ対策等については、技術が日進月歩であること等を踏まえるとガイドラインに記載することは妥当ではないとの意見が多数示された一方で、参考となるセキュリティ対策の例を示したり、認証紛争解決事業者のモデルとなるような規程の一例を示したりするなど、ガイドラインの見直し以外の方法で情報提供する方策も検討すべきでないかとの意見も示された。

この点に関しては、今後予定されているODRにおけるセキュリティ全般についての検討も踏まえつつ、事務局において更に検討を進めることとしたい。

