参考資料７－３

# 組織が発行するデータの信頼性を確保する制度に関する検討会（第６回）

１　日　時

令和２年 11 月６日（金）10：00～12：00

２　場　所

WEB 会議による開催

３　出席者

（構成員）手塚座長、宮内座長代理、新井構成員、伊地知構成員、岡田構成員、小川構成員、小木曽構成員、小田嶋構成員、小松（博）構成員、柴田構成員、渋谷構成員、袖山構成員、中田構成員、中村構成員、濱口構成員、山内構成員、若目田構成員

（プレゼンター）GMO グローバルサイン株式会社漆嶌氏

（オブザーバー）小島内閣官房情報通信技術総合戦略室参事官補佐、青木金融庁総合政策局総合政策課フィンテック室係長、朝山法務省民事局商事課課長補佐、布山経済産業省商務情報政策局総務課情報プロジェクト室室長補佐、尾崎経済産業省商務情報政策局サイバーセキュリティ課課長補佐

（総務省）田原サイバーセキュリティ統括官、藤野サイバーセキュリティ統括官室審議官、中溝サイバーセキュリティ統括官室参事官（総括担当）、高村サイバーセキュリティ統括官室参事官（政策担当）、海野サイバーセキュリティ統括官室参事官（国際担当）、高岡サイバーセキュリティ統括官室参事官補佐

４　配布資料

資料６－１　GMO グローバルサイン株式会社提出資料

資料６－２　株式会社コスモス・コーポレイション提出資料

参考資料６－１　データ戦略タスクフォースの開催について

参考資料６－２　トラストサービスの現状と課題

参考資料６－３　組織が発行するデータの信頼性を確保する制度に関する検討会（第5回）議事要旨

５　議事要旨

（１）開会

（２）議題

①関係者ヒアリング

漆嶌氏、濱口構成員から資料６－１、６－２について、説明があった。

②意見交換

主な意見は以下の通り。

袖山構成員：EU 適格証明書の有効期間と更新時の手続について具体的にご教示いただきたい。

漆嶌氏：更新の事例がまだないため、説明が難しい。有効期間は２年未満と記憶しているが内部で詳細を確認し事務局経由で回答させていただきたい。

袖山構成員：有効期間が１年から２年程度であるということ、更新手続は有効期間が切れているものがないため回答ができないということについて承知した。

また、国際相互運用性のある e シール用証明書の検討にあたり、国税庁が管理している法人番号が利用できるのではないかという話があったが、消費税のインボイス制度の開始に伴い発番される適格請求書発行事業者の登録番号の情報を拡張領域に追加するようなことも可能と考えてよいか。

漆嶌氏：拡張領域に日本独自の拡張を加えるというのは、国際相互運用の観点からは適切な方法ではない。その代わりに証明書の主体者名、発行先の会社名のフィールドに様々な情報が格納できるため、そこにインボイス用の情報を書き加えるというのが相互運用性の観点からは適切なやり方ではないか。

小田嶋構成員：資料６－１の５ページにある、e シール用適格証明書の発行に当たって行う実在性の確認はかなり厳格だと思っている。GMO グローバルサインのポリシーなのか、eIDAS なのか、ベルギーの国内法なのか、この手続の根拠について教えていただきたい。EU の各国でこれが一緒なのか、違うのかというところも可能であればご教示いただきたい。

また、資料６－１の８ページに関連するが、外国法人に関しても一定の手続を踏み、一定の条件を満たせば法人番号を指定できる。この点は念のため補足させていただく。

漆嶌氏：審査方法やその基準というのはベルギー特有、弊社独自のものではなく、EU 共通で監査されている内容であると考えている。グローバル企業の監査法人による監査を受けているため、他の認証局に対しても同様の水準の手続を踏んでいると認識している。

柴田構成員：１つ目は、eIDAS の規則では、e シールの用途として、ドキュメントの発信証拠とデジタル資産の認証の２つが書かれているが、証明書発行側としてはそうした用途の区別をしているのか。

２つ目は、自然人の場合は署名鍵を使う方がその鍵を管理する特定の個人に固定されている一方で、組織の場合はその署名鍵を使用して署名する主体が組織に属する複数人であったり、組織が運用するプログラムであったりすると思うが、発行側として証明書の利用に関して義務規定などを用意しているのか、また eIDAS 等に規定があるのかという点について教えていただきたい。

最後に、e シールが eIDAS の規則に入れられるに至った経緯について、何か御存じであれば御紹介いただきたい。

漆嶌氏：１点目について、利用の方法としてアセット、エビデンスが考えられるという話があったが、自社も含め e シールの発行事業者の証明書を何社か確認したところ、基本的にはドキュメントの出処の証明しかしていないということが分かった。ドキュメントのデジタル署名専用の証明書ということで、コード署名とかそういった用途には使われていない。コード署名用に eIDAS ベースの証明書が使われているかどうかといったことに関しては、現状ではまだ事例がないと理解。

２点目のトークンの管理の仕方に関しては、USB トークンをお渡しした後、制限された管理者の中で適切に管理してくださいという同意書を結ぶことでそれを担保しており、その同意書の範囲の中で各企業に管理をしていただいている。

宮内座長代理：USB トークンのコピーの可否についてはどういうルールになっているか。また、トークンの管理の仕方については、制限された管理者の下で適切に管理するというレベルだと理解したが、適格電子署名の場合と概ね同じ規定だと考えてよろしいか。

漆嶌氏：トークンの中からは秘密鍵を外に出せないため、証明書１枚につきトークン１個で、鍵の複製はできないということになっており、複数人の管理者の中で共同利用いただくということになっている。２点目についてはおっしゃるとおり。ただ、自然人は署名鍵を誰かに渡して署名してもらう、というケースは考えにくいが、法人の場合はその管理の中で考えられるということで、「適切に管理」のレベルが変わってくると認識している。

手塚座長：USB トークンといった場合は、耐タンパ機能がある USB トークンという理解でいいか。

漆嶌氏：おっしゃるとおり。認定を受けた耐タンパデバイスである。

渋谷構成員：法人の実在性確認にあたって、具体的にはどのようなドキュメントを基に審査をされているか。国内ビジネスにおいては個人事業主を対象にされているところもあると思うが、何が審査の基準となっているドキュメントか教えていただきたい。

漆嶌氏：現時点では、日本向けに e シール証明書発行サービスは提供できていない。トライアルで JIPDEC 宛に発行した証明書を例にとると、審査の具体的な内容は、まず法人番号の登録があるかどうかについて申請書と法人番号のサイトで一致の確認をした後、弁護士や公認会計士等の正式な第三者の検証者と対面で確認を行ったという手書き署名の、同意書を確認した上で、発行させていただくという流れになっている。

山内構成員：JIPDEC は適格 e シールに必要な適格電子証明書を GMO グローバルサインのヨーロッパの認証局に発行してもらい、USB トークンに格納して昨年末に御提供いただいている。有効期間は１年であるため、今年の 12 月にその期限が来ている。

漆嶌氏の説明に補足すると、私が実際に役員であるということを証明するために、運転免許証のコピー等をお渡しし、対面確認では、山内という人間が JIPDEC の役員であるということをご確認いただき、弁護士にサインいただいた。

主な利用シーンとしては、JIPDEC の執務室の中で作る一部の PDF に e シールを付している。USB トークンを執務室でしっかりと管理する必要があるため、執務室に出勤しなければ e シールを発行できないというのが現状であり、テレワークに対応するのは難しい。これから大量に e シールを発行することを考えると、クラウドサービスなどを使って、リモートで e シールを発行するということが必要だと思う。ただ、日本国内ではまだ e シールの仕組みすらないので、この検討会においては USB トークンによる e シールの発行を端緒として、最終的には、リモートで e シールを発行できる仕組みを実現していくことが重要だというのが現場サイドでの所感。

手塚座長：e シールの発行に必要な証明書を USB トークンに入れて運用すると今いただいたような問題がある。他方、ヨーロッパでは、証明書を HSM に入れてサーバー型で運用する方法も実現していると考えてよいか。

漆嶌氏：弊社でもリモートクラウド型の署名については対応を計画中であり、実装等を進めているような状況である。他社を見るとクラウドで行うようなサービスもあったように思う。法律上、やれない話ではない。コロナ禍の現状を鑑みると、そうしたリモートクラウド型の署名の重要性は増していくと思う。

新井構成員：１つ目はデータの起源と完全性を保証するために用いられるのが e シールという説明があったが、法人が主体のときには意思ではなく起源が用いられるのは何か理由があるのか。欧州での背景などあればあわせてご教示いただきたい。

２つ目は、証明書のサブジェクトのところに日本語を入れることができるかどうか。サブジェクトには、国際流通、相互認証の観点から一般的には 26 文字分アルファベットや数字を入れることができると認識しているが、欧州ではウムラウトがつくドイツ語等の英語以外の言語も入っているのか。

また、適格ではない e シールについてはどういう状況にあるのかをお聞かせいただきたい。適格にこだわり過ぎて厳しい仕組みになってしまうのではなく、e シール普及の観点で考えると非適格の e シールも必要で、そちらのほうは欧州でも検討をされているのかという点が気になっている。

漆嶌氏：１点目については、私から御説明するよりも法律の専門家の方から御回答いただくのが適切だと思うが、私見としては、実際に手書き署名をする法人の場合は、文書の出処というか、起源のところを示すだけで、内容について同意したとか主張したとかといったことはないという理解。

２点目については、日本語を入れた EV 証明書は、国際相互運用の観点から英語名についても併記するような形でやっていたケースがあるため、そういった対応になるのではないか。また、ラテン文字等でウムラウト等がつくようなケースがあり、今いただいたような要望はマーケットから実際にいただいており現状は対応を検討しているといった段階。

３点目の適格ではない法人の代表者、組織向けの証明書というのは発行しており、例えば S/MIME やコード署名といったところで御利用いただいていて eIDAS の中で何か網をかけるといったことは特にないと認識。

濱口構成員：３点目について補足すると、適格というのは、法的要件を全て満たし、即座に法的効力が認められるトラストサービスを指している。非適格や先進というのは、全くの自由市場であり、先進 e シールであるための基準というのも定められていない。フォーマット、推奨アルゴリズムや推奨パラメーターはあるものの鍵長やアルゴリズムがこうではないといけないというものはなく、明確にこれが先進電子署名といえるための基準はない。

他方、適格の制度が構築されたことにより、適格のための技術基準、適格のための監査制度というのは出来上がっている。そのため、欧州の認証局は、適格のサービスを提供している一方で、同じ認証局の環境を使った非適格のサービスについても提供している。技術的には適格と同等でも、本人確認の要件が軽くなっていたり、例えば最後にＩＣカードの中に秘密鍵を入れずに渡していたりといった点で適格のものと差異があるサービスである。そのため、適格の制度ができたことによって、非適格のサービスに関しても、基準が明確になってきているといえる。

宮内座長代理：１点目に関して、法人は意思表示ができないため、意思という言葉を使わないというのは、日本でもヨーロッパでも同じだが、起源という訳語の原文であるオリジンに立ち返り、発行元とか作成元といった訳であればそれほど違和感はないのではないか。

中村構成員：資料６－１で、適格証明書でも一般的な PKI のものと技術スペックという意味では変わらないという言い方をされていたが、署名のフォーマットとしては、PKCS７や S/MIME を一切排除し AdES 中心にやられているということで、セキュリティ上の理由かもしれないが排除した理由、仕様上排除せざるを得なかった理由について伺いたい。

漆嶌氏：AdES と CMS や PKCS７等の一般的な署名フォーマットの違いは、署名者の証明書をしっかり特定できるようになっているかという点と、タイムスタンプを付与するための標準が整っているかどうかという点の、２点にかかっていると思う。それがあれば、ほかのフォーマットであっても AdES 相当になるため、その後適格署名にできるが、反対にその機能がないと適格となるのは難しい。

濱口構成員：必ずしも AdES フォーマットでなくても、適格の要件を満たすことはできる。他方、加盟国の公的機関が受け入れるものに関しては、フォーマットが指定されているという状況であり、そのフォーマットの中心となっているのが AdES である。公的機関が、例えば、市民から確定申告のオンライン申請を受け付ける場合には、AdES のフォーマットでしてくださいという形。

中村構成員：各公的機関からすると方言等の排除という意味で指定せざるを得なかったと理解。

小松（博）構成員：資料６－１について、e シールに関するサービスの CP/CPS が外部に公開され利用されているかどうか、また日本語による CP/CPS があるかどうか教えていただきたい。

漆嶌氏：日本では、正式に e シールの販売のサービスが始まっていないため、英語版しか公開されていない。英語版については、ウェブサイトを

確認すれば確認できる。

高村参事官：最終取りまとめをどういう方向へ持っていけばいいかという観点から考え方を伺っておきたい。

先ほど別の AdES フォーマットが規定されればそれを使用して、EU における適格署名にはなり得るという話があった。例えば日本国内で現在使われている PDF に対する電子署名であれば ISO の 32000 で規定されている電子署名の方式を使っている。それに対して ETSI 側は PAdES という形で拡張した形のフォーマットを選び、32000 と合致していないため、32000-2 として国際標準化する必要が生じた。

資料６－１にあるように欧州 eIDAS における e シール用適格証明書のフォーマットが RFC 5280 ベースでできているという話があるが、これを突き詰めていくと、RFC 5652 CMS というもので電子署名を含めた、PKI などを使ったデータのやり取りのためのフォーマットが決まっていたところに別のフォーマットである RFC 3739 QC プロファイルが作られたという流れ。

一方で、日本データ通信協会で認定されているタイムスタンプは RFC 3161 で標準化されており、RFC 3739 とは整合はしていない。要するに、欧州側が新たなフォーマットを eIDAS に伴って投入し、既存の国際標準にとらわれない形で規格をつくり、それを国際標準化しようとしているというのが現状と理解している。

他方、日本に枠組みが存在していない e シールについては、どの標準を選んでもいいという状況になっている。通関手続等のユースケースを想定し、既存の電子署名やタイムスタンプとの整合性を棚上げし、欧州と完全にコンパチブルな形を目指すほうが適切か、それとも、e シールと電子署名で確認に必要な技術を切り替えなくていいように、既存の電子署名との整合性をまず取り、国際相互流通の担保に必要な部分は、機械的に変換可能な、コンパチブルな形で埋め込む方が適切か、どちらの方向性が適切かというのを皆様方にお考えいただかないといけないと思っている。ぜひその旨、頭の片隅に置きながら、皆様方に御検討いただければ非常にありがたい。

手塚座長：次回以降の論点として議論していくということで整理させていただく。

山内構成員：ヨーロッパのように、一般的なトラストサービスプロバイダーの技術基準、さらに電子証明書を発行する認証局の技術基準という形で決めて、その中で発行対象が人なのか、法人なのか、モノなのかという形で分けていく、そういった整合性がある仕組みを日本でも検討す

べきだと前々から申し上げている。

濱口構成員の説明の中で電子署名法には技術基準だけ欠けているという指摘があった。具体的に申し上げると、現行の電子署名法に基づく認定認証業務の技術基準は 20 年間ほとんど改正されておらず、HSM の基準も FIPS140-1 に基づいて作られており、現行はほとんどの事業者が FIPS140-2 に移行済みだという状況を考えるともう古い基準になったと言わざるを得ない。タイムスタンプ認定制度における検討会においては、FIPS140-2 のレベル３認証相当以上というのが、議論されていることを考えるとトラストサービスを横串で捉えて、現行の電子署名法を活用していくようなことであれば、現行の電子署名法の認定制度における技術基準についても見直していく、そういう時期に来ているのではないか。

小田嶋構成員：濱口構成員に２点質問がある。資料６－２の 13 ページ目のスライドで、証明書を発行する認証局に求められる法人の確認方法の要件と日本の電子署名法の認定認証業務の本人確認の要件に大きな違いがあるということだが、それ以外に違いがないかということを確認させていただきたい。

２点目は、資料６－２の６ページ目で、現状、ナショナルレジスターという意味で言うと、法務局の法人等番号と国税庁の法人番号の２つあると思っている。これらを明示的に区別して表示するといった場合、どのような方法があるか。

濱口構成員：１点目の認証局の要件だが、RA の本人確認、法人の確認以外にも、日本で要求されていないものというのは多数あり、例えば財務上の安定性や廃業時の計画等がある。また、日本で要求されている部分でも、欧州の要件とは少しずつ差異というのは存在する。ただ、今回の説明では、時間の都合上割愛させていただいた。

２点目は NTR についてだが、法務局の法人等番号と国税庁の法人番号が、日本ではナショナルレジスターとしてあるという考え方は２つあるかと思う。今回、e シール用の証明書に書く識別子として、NTRJP として法務局を採用するか国税庁を採用するかという、どちらか一方を採用するというのが１つの考え方。

もう１つは、ローカルスキームとしてこの２つを提示するということが考えられる。例えば法務局の法人等番号であれば、ミニストリー・オブ・ジャスティスなので、「MJ：－識別番号」、国税庁であれば、タックス・エージェンシーなので「TA：－識別番号」というような運用も可能かと思う。

③　その他

事務局から、次回の日程について説明があった。

（３）閉会

以上