

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4回）

1 日 時

令和2年8月3日（月）16:00～18:00

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、小木曾構成員、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

（ヒアリング対象者）xID株式会社日下氏

（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、山本内閣府政策統括官（科学技術・イノベーション担当）付上席政策調査員、朝山法務省民事局商事課課長補佐、三輪金融庁総合政策局総合政策課フィンテック室長、手塚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4-1 一般社団法人新経済連盟提出資料（非公開）※

資料4-2 xID株式会社提出資料（非公開）※

参考資料4-1 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3回）議事要旨

※資料調整後、後日総務省HPにて掲載

5 議事要旨

（1）開会

田原サイバーセキュリティ統括官他から挨拶。

（2）議題

①関係者ヒアリング

小木曾構成員、日下氏から資料4-1、4-2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。

小田嶋構成員：資料4-1の3ページ目の事例、複数企業がまたがったEDI等でのeシールの活用について、コメントしたい。EDIは親企業が中心となるハブ的な使い方が多く、各企業が親企業ごとにEDIシステムを使い分けているといった状況にある。これがネックとなっているため、EDIを相互接続してメッシュ型と呼ばれるような仕組みとし、1つの組織が1つのIDで識別可能とすべき。そのときに、各EDIから個々の組織が発出するデータの発出元証明としてeシールを活用できるのではないかと。業務のDXやペーパーレス化にもつながる。

資料4-1の6ページ目についてもコメント。法人のデータとeシールの見える化で、民間の企業のデータベースなどを援用できれば様々な属性を使った見える化ができるようになり、SDGs等の取組目標などもeシールに表示できる。

山内構成員：最近のEDIは、製造業、流通業、建設業等において企業間の受発注データを専用回線でやり取りするものから、インターネットを使うものに変化してきている。インターネットによる通信の相手先が本物であることを確認するため、通信を行うパソコンの端末認証に関する検討が、インターネットEDI普及推進協議会で行われている。これは従来型の受発注データのEDIなので、電子署名やeシールからは少し距離がある。

ただ、クラウド会計ベンダーによると、企業間の契約書、請求書あるいは領収書などの取引文書を電子化して活用するのも、インターネットEDIと呼ばれてきている。受発注データと、請求書、領収書、そして契約書の電子化の全体を捉えた上で、インターネットEDIをどのように活用していくかというのは政策的課題。

また、EDIで使われるデータを第三者に対して提供する場合は、法人の真正性を示す証としての日本版eシールのようなものが重要かもしれない。電子インボイスとインターネットEDIについて、関係省庁に政策の方向性を聞いてみると、EDIに関連した日本版eシールの役割が分かるのではないかと。

小松（博）構成員：資料4-1の4ページの中で説明があった監査法人の対

応について補足したい。AIやデジタルのデータを活用した監査というのを現在進めている。特に、eシール等とはあまり関係がない内部のデータを使った監査という観点で議論が進んでいる。出荷データ、検収データ、請求データや入金データ等の企業が作成したデータの突合や分析による異常の有無をAIで検証するといったことをシステムで行うため、基本的には内部で作成したデータ自体を活用するという形であり、eシールや電子署名といった話にならない。

ただ、リモートでデータをやり取りする機会が増え、真正性をどのように担保していくべきか、という話はまだ議論できていない。eシールの制度がより深く広く普及していけば、eシールを活用しようという話になると思う。個人的な意見だが、eシールという仕組みについてユーザーとなる企業の方の理解を得たり実際に使ってもらったりすることが重要。

柴田構成員：eシールの付与された情報が様々なところに流れていき、将来その情報を利用する方がしっかり検証できるということが重要。そのために、発出時の情報が正しいということを担保するトラストサービスが必要になる。標準化や制度化を進め、利用者が使いたいときに使えるようにすべき。

袖山構成員：登記情報が公開されているため、エストニアではeシールの発行が非常に簡単だというお話があった。一方で、日本においてeシールを発行する場合は代表者の本人確認等があり、非常に煩雑だったと聞いているが、実際のところを伺いたい。

また、日本版のeシールが制度化された場合には、法務省の登記情報のオープン化や既に運用が開始されている国税庁の法人番号サイトをAPI連携し活用することも想定できるのか。

エストニアの場合、登記されていない者をeシールの管理権限者に登録する場合は、電子委任状によって簡単に設定ができるとある。日本においても電子委任状法があるが、そこでは認定認証事業者の電子署名が必要となり非常に手間がかかるものと認識している。eシールを幅広く普及させるためには、消費税のインボイス制度への対応といったユースケースに加えて、eシールの取得や運用が容易いことも重要。取得や運用のしやすさにおいてはeシールの鍵管理がポイントになるだろう。

日下氏：2つ目の国税庁のAPIのところに関しては他に適任者がいると思う。個人認証に関しては、エストニアでは基本的に日本でいうマイナンバーカードに限定されている。普及率99%であるマイナンバーカードと

同等のIDカードに入っているICチップ内の電子証明書と秘密鍵を使って電子署名をするという形で身元確認をやっており、鍵管理の使いづらさ等は特にはない。何か特定の認定認証事業者に限定したサービスを利用しなければならないわけではなく、無償で発行され、国民ほぼ全員が持っているIDカードを通してオンラインで認証ができるため、日本で同じことをやろうと思うとシンプルにマイナンバーカードの普及に尽きると思う。

エストニアの場合には、SK ID Solutionsというeシールを発行している企業がスマートIDという民間IDアプリを提供している。このサービスによりIDアプリで鍵管理ができる。もっとも、eシールに関してはメジャーで使われているのはUSB型を提供しているCryptstickであり鍵の管理は現実世界での管理になってくる。ただ、一部の業者で、eシールの鍵管理自体を個人認証の自分が持っているIDカードの秘密鍵を使って行うといった話というのは出てきている。ただ、これを実際日本でやろうとすると、かなりハードルは高いと思う。

濱口構成員：現状の認識を確認したい。エストニアのデータ連携基盤、X-Road上での情報交換というのはセキュリティサーバを介して行われる。そして、X-Roadにつながっている各情報システムのオーナーである組織、すなわちX-Roadのメンバーのeシール用証明書がセキュリティサーバに保管されており、X-Road上で実際に情報交換を行う際には自動でeシールが付与され、検証されていると認識。データ連携基盤、X-Roadの実現のためのコアな要素としてeシールが使用されており、年間で12億件ほど情報交換されていると思うので、エストニアというのは最大のeシール利用国ではないか。

日下氏：弊社でもX-Roadに接続した法人登記サービスというものをデジタルIDと連携してやっているがeシールは使っていない。ただ、例えば電子処方箋や医療データのカルテについてはeシールが使われているものもある。ガードタイム社が提供しているアーカイブ式のタイムスタンプや日本でいう認定タイムスタンプのようなもの、eシール、ウェブ証明書的な証明書も含め、大きく分けて4つのトラストサービスが複合的に使われている形であるため、eシール自体の単体のトランザクションというのは手元にデータがないが他国、同じ規模のGDPの国などと比べると圧倒的に多いとは思う。全てのデータトランザクションにeシールが使われているわけではないと認識している。

濱口構成員：X-Roadの仕様を読むと、全部つくような形に書かれていたが、実際はそうではないということか。

日下氏：それはdigital time-stamping signatureとなっているか、それともeシールと書いてあるか。

濱口構成員：具体的にはe-stamp certificateである。ただ、eIDASのAnnex IIIを参照しているためeシール用証明書と認識している。eシール用証明書を参照した、SK IDは、X-Roadの仕様上はe-stamp certificate、electric stampと呼んでいるがeシールそのものだと思う。X-Roadに接続するセキュアサーバのところである。

日下氏：現状、我々もX-Roadに接続はしているがSK社からeシールを取っているわけではない。ただもう一度私も確認する。

小田嶋構成員：資料4-2を見ると、レジストリーコードとVATナンバーは識別子として使われている。識別子があれば、経理部門によって行われる消し込みといった手続きの自動化もできると思う。例えば実データとeシールを照合して住所が不一致だったとしても、その識別子があることで、様々なデータベースを援用して最新のデータを自動確認して、自動消し込みもできると思う。また、プレゼンいただいた融資審査資料、収入証明や残高証明の利活用というのはとてもよい事例だと思う。

柴田構成員：自然人の場合は、1つの署名鍵とこれに対する証明書があり、当事者のみがアクセスすることで本人性を担保している。他方で、eシールの場合は1つの署名鍵に対して複数の方がアクセスすることになると思う。セキュリティサーバにアクセスする際の制限や規約があれば教えてほしい。

日下氏：弊社で使用しているSK社から発行されるCryptstickはいわゆるUSBリーダーなので挿した後にIDカードで認証する。事前に認証するというか、権限者として私のIDカードが指定されていれば、それでアクセス管理ができる。そのため、他の人間がCryptstickを挿して、他のIDで認証しようと思っても、権限者として指定されていなければできない。ただ、これは全社的に、例えば制度とか法律でそうなっているとかいうわけではない。企業ごとのコンプライアンスや保管のルール次第。全社を見ている訳ではないため、確実なことは言えないが、自社で見たフローとしては誰がいつCryptstickの中にある署名鍵にアクセスしたのかというアクセス管理というのはID認証ベースでできている。

新井構成員：まず、電子署名とeシールはエストニアではどう使い分けられているのか、実際はつきり使い分けられているのかというところを教えてください。2点目は、電子署名はICカード、eシールはCryptstickのようにデバイスに関しても規定があるのかという点。3点目について

は、eシールを出すための電子委任状には何か決まった項目やフォーマットみたいなものがあるのかどうかというところについて教えていただきたい。

日下氏：電子署名とeシールでは個人認証と組織認証というところで根本的に違いがある。エストニアにおいても電子契約では基本的に代表者同士の個人の電子署名で企業同士の契約として法律的に認められている。他方で、組織の代表者ではない人間が取引をする場合に、双方とも組織が正当に発行した書類であることを証明できない場合や、不正により損害を被るリスクがある場合はeシールを活用することがある。ただ、電子契約においてはeシールより電子署名の方が一般的である。商業登記データベースに役員情報が全て記載されているため、それを参照すれば、その人が署名権限者なのかどうかというのは、基本的には役員クラスであれば分かる。代表者以外の方であれば、電子委任状を書いていただく、代表者の電子署名つきのファイルを共有していただくといったことが実際の現場におけるオペレーションである。

2点目だが、eシールのデバイス規定は、耐タンパー性のあるハードウェアに限るといった規定がエストニアとしてあるわけではない。Cryptstickも発送コストと製造コストがかかってくる部分があるので弊社でもデバイスについてはユーザビリティの観点で検討中。

3点目について、電子委任状のフォーマットには特に制限がない。誰がどういった行為を委任するのかということが電子委任状に記載され、電子署名がされていれば、商業登記を確認しに行くことで代表者の署名がされているのかというのがどうかを確認できるため、それで問題ないという形であり、項目等の規定は特にない。ただ、SK ID Solutions社が用意しているテンプレートを使う社が多いと思う。

新井構成員：フリーフォーマットとなると目視で確認することになるか。

日下氏：ドキュメント自体は、PDFに個人認証の電子署名をしたものがアップロードされ、内容自体は目で確認する形であり、マシンリーダーンにして自動的に処理しているというわけではない。エストニアではPDF形式ではなく、そもそもASiCというフォーマットであり、XMLとなる。そのため、PDFに電子署名してコンテナファイルにするのではなくエクセル等の他のファイル形式にも署名できる。PAdESと違う形式であるため内部的にSK社がマシンリーダーンにしようといった話をしている可能性はある。

新井構成員：代表者のeIDの電子署名とそもそも商業登記というのはひもづいているか。

日下氏：エストニアの会社法上、代表取締役という概念がないものの、役員に関しては商業登記に記載がある。商業登記側にはIDカードのID番号まで全て記載がある。そのため、そういった意味では、ひもづけは可能。ただ、日本における代表取締役のような者は登記上存在しないため、そこまでの把握をする必要がないというのが正確かと思う。

宮内座長代理：商業登記データベースのオープン化だが、もう既にAPI化しており、手続をすればAPIの仕様も見られるようになっている。そういう意味でオープン化は進んでいるが、見られる情報が非常に限られているということが問題。代表者は住所まで見られる一方で、代表者を除く役員については氏名しか見られない。氏名以外の情報については、利害関係者であることを証明して閲覧することができるというルールになっている。また、代表者の住所についてもプライバシーの観点から一般公開はやめるべきであるという意見の人も結構いるようで、エストニアのように自動車のプレート番号から全部情報が見られるとか、そういうオープンな国とは随分やり方が違うなと思っている。法務省の方からコメントがあればいただきたい。

法務省：商業登記の関係は担当ではないためお答えするのが難しい。

山内構成員：JIPDECは、法人の実在性及び属性に関する共通基盤として、サイバー法人台帳ROBINSを進めてきたが、一法人が企業データを集めてきて世の中の基盤にするのには大きな壁があるということで、昨年度末で終了した。根本的な国の仕組みとして、法人の実在性に関するデータは、デジタル化・オープン化されるべきであると思う。エストニアの例などを参考にして、プライバシーとの関係も整理した上で、eシールの普及が目的ではなく、法人の実在性の重要性を皆が認識し、それに基づくデータ連携ができるような仕組みを大きな枠組みで考えていただきたい。

岡田構成員：法人データの見える化でサービスを創出というのはeシールを普及させる上で一つのキーになると思う。エストニアでは駐車している車の情報やナンバープレートの情報、事故情報もオンラインですぐ見られるということだが、プライバシーとの関係性はどのように捉えられているのか。

日下氏：エストニアのデータ連携基盤でやり取りするデータは、データを開示する側とアクセスする側の双方が個人認証して、いつ誰がどの情報にアクセスしているかというのがしっかり記録されている。その意味で、基本的にオプトイン形式である。ただ、事故情報に関しては警察の扱いとなり、特別扱いされていて、オプトイン形式ではなく、一般開示

されることになっている。

高村参事官：日下氏から御説明いただいたエストニアのeシールについては、使われ方が、日本の商業登記上の商業登記電子証明書の使用方に限りなく近いと思う。証明書の申請自体が電子完結しているかどうかという部分、もしくは委任状が必要かという部分は別にして、証明書自体の位置づけというのは限りなく近いのではないか。

組織としての署名ということを前提に皆さんに御議論いただいているものの、果たして本当に組織による署名というのが必要なのかというのがまだ分っていない。自然人であれば、極めて法的に例外的な状況がない限り戸籍情報というのは変わらないわけで、その存在自体が変わることはほぼないだが、組織の場合、特に企業の場合、頻繁に組織変更される。新しく部署ができる、もしくはカンパニー制に変わると言っただけで組織の名前がころころ変わり、多ければ年に1回、組織の名前変わったと名刺をお持ちになる方がたくさんいるというのが実態かと思う。そうしたとき、果たして追跡性という意味で組織による電子署名というのにどこまで意味があるのかということを感じている。

また、資料4-1の15ページで、押印されたものが実印でない、認め印である場合、二段の推定が及ぶことは難しいというところに赤線を引いていただいているが、果たしてこういったものについて、要するに、その押印したエンティティが何なのかというのがよく分からない、組織によるデータの信頼性とは果たして何なのかというのが正直よく分からない。

欧米の方々と契約を結ぼうとすると、相手が会社であろうが誰だろうが、マネジャーなり何なりの権利を委任されている方の個人のシグナチャー、電子署名ではなくて、物理的なサインがなされている契約書が取り交わされることが通例だと考えている。そういうことを考えていったときに、日本の商習慣の中で存在している、組織により取り交わされる紙というのは果たして何なのだろうか。それについて果たして真正性、信頼性というのをどこまで担保する必要があるのかというところを皆さんどうお考えなのかというのをぜひ御教示いただくと大変ありがたい。

宮内座長代理：そもそもeシールというのは契約に使うべきではないと思う。いわゆる法的な意思表示には使わないという前提で、そうでないものについて、発信元がどこの企業であるかというのが原則的な使い方。そのため、企業内の組織ではなく、企業や法人という意味での組織の認証、出元の確認というものに使うのが第一義。その上で、組織としてこうい

うことを認めているという事実の通知を行うケース、請求書のようなものに用いられるのが主なeシールの用途ではないか。発信元が分かればよいのであり、代表者あるいは代理人の意思表示をするものではない。個人名の記載はなく、証明書はあるウェブサイトの認証やプログラムに対するコード認証に近く、様々な文書をここから発行したというような意味で出すのがeシールだと思う。

日下氏：eシールについては個人的にもまだ疑問があるものの、eシールの用途は意思表示ではなく発行証明の部分なのかな、と思いエストニアの事例を紹介させていただいた。弊社はもともと2013年から主にブロックチェーン関連の事業を専業でやっていく中で、一番大きな課題感が個人認証の部分だったため、デジタルIDを中心に進めてきた。

法人の認証というところであれば、例えば航空会社が遅延証明書をeシールつきで発行することで遅延保険が組めるといった話もこれまではブロックチェーンでやろうとしていた。しかし、データ自体がブロックチェーンの外側で生まれた場合に、本当にそのデータが正しいデータなのかというのを純粹にAPIだけでやる、あるいは、複数の情報の出どころから取ってくるみたいな形でオラクル問題を解決するという話はあったものの、一つの方法論として、発行証明へのeシール利用とブロックチェーンでのデータ活用みたいのところというのはすごく可能性があるのではないかと。今まだ分散型のデータソースから確からしい中央値を取ってくるというやり方は難しいため、そういった意味では、信用あるエンティティの情報の信頼性をより担保してあげてデータインセットに使うというのはすごく可能性があるのではないかと考えている。引き続き、何か機会があれば議論に参加させていただきたい。

高村参事官：組織と言っているのが、法人もしくは権利能力なき社団といった主体が中心ということであれば、かなり論点を絞ることができると思っている。商業登記証明のような認証の程度が重いものに対してもう少しカジュアルなものについて、こういうときにこういうものを使うと、こういうメリットがあるというガイドラインのようなものを整理できると、皆様方に使い勝手のいい何かが出来上がる気がする。あとは、その部分について、国が強制するのか、後押しするのか、それとも、こうあるべきじゃないかという提言で止めるのか、というところは検討が必要だが、もともと総務省は可能な限り全てオンラインであってほしいと考えている役所であるため、ぜひとも皆様方の御協力を賜りながら、少しでもいいものを取りまとめることができればと思っている。

- 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