参考資料 11－１

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 10 回）

１　日　時

令和３年３月５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、小川構成員、小木曽構成員、小田嶋構成員、堅田構成員、小松（文）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

（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）上席政策調査員、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、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 10－１　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 10 回）事務局資料

資料 10－２　富士通株式会社提出資料

参考資料 10－１　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９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

事務局から資料 10－１について、渋谷構成員から資料 10－２について、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 10―１の３ページに、識別子については Object Identifier を軸に今後検討とあるが、民間の法人の場合は基本的に有料で取得するものであり、新規だと２万円、３年ごとの更新に１万円がかかる。Object Identifier は e シール用電子証明書を発行する CA が自身をワールドワイドで一意に識別できるようにするというのが本来の使い方であり、e シール用電子証明書の発行に際して利用者側にこのような手続が必要となるとすると、煩雑であり取得に後ろ向きになる懸念がある。識別子等は複数あるが用途に応じふさわしいものが選択されると思う。無償で利用できる法人番号や適格請求書の発行事業者登録番号、加えて民間の事業者の番号などを軸としてはどうか。OID と書くと、Object Identifier と Organization Identifier との混在に気をつけなければいけないが、識別番号の格納に関しては、Organization Identifier、OID でいう２．５．４．９７が相応しいと想定している。電子署名法の認定認証事業者も Organization Identifier に法人番号を入れている事例がある。

７ページ目について質問で、レベル２の e シールであっても第三者による評価を受けている場合は、評価を行った第三者機関を拡張領域に記載することを認めるとあるがこれはどのような内容を想定しているか。第三者機関に定義がないと有象無象の機関が乱立し、その結果ユーザーが混乱することがないかと懸念をしている。

最後に、９ページ目・11 ページ目の記載に関しては賛同。

事務局：第三者機関は調査機関のようなものを想定しており、例えばドイツだと TüVIT、日本では電子署名法の指定調査機関である JIPDEC やタイムスタンプの制度を運営する日本データ通信協会がある。このような機関から認証を受けているような場合、その旨はレベル２の e シール用電子証明書の拡張領域に書いてもいいということ。

第８回で濱口構成員・渋谷構成員から欧州の状況の説明があり、先進のレベルの e シールに関しては、任意で第三者認証機関の認証を取得し、その場合は第三者認証機関がサイト等で公示するという話があったということも参考にしている。

OID について、本検討会で詳細を議論する予定はないが有料の場合もあれば、総務省の指定・管理するもののように無料であるものもあると記憶している。今回は、法人番号、適格請求書の発行事業者番号やその

他の民間企業の番号等複数の番号体系がある中で、本検討会において一つに決めることは難しいため包括的にID番号を書けるような書き方はどうかということでお示ししている。Organization Identifierについても、オブジェクト識別子での書き方の一つのアプリケーションサンプルではあると思うため、その利用も将来選択肢に入ってくると思うが現段階では、幅広い番号体系を書けるような形を取っておくということが重要ではないかということをまずは合意しておきたい。また、９ページ、11ページへの賛同の意見は非常にありがたい。

小田嶋構成員：監査機関を拡張領域に書くというのはレベル２の宣言にもなるともいえ、識別の在り方としてはいいと思う。また識別子についても現段階の考え方を承知した。

手塚座長：国際的な相互承認をやるときにも融通するような番号体系を念頭に置くのはもちろんだが、国内だけで流通するものだったら国内では信頼のある番号体系で十分という考え方もでき、全ての e シール用電子証明書に格納する識別子について国際間で流通するような体系にまで持っていく必要があるかどうか、その辺の拡張性を含めて論点整理していくということが大事。

新井構成員：資料10―２の２ページ目、欧州ではFIPSからISOへ移行しているとあるがそのポイントや背景は何か。３ページ目について、ISO/IEC 15480を利用するということは認定要件となるPPが必要になるが、本検討会で検討するｅシールの制度においてはどのようなPPがふさわしいのか。欧州のPPをそのまま使用するのか、それとも日本独自で作成する形がいいのかというところについても伺いたい。前回私が質問した e シールを付与する際の代表者の意思について７ページ目の３点目に盛り込んでいただきありがたい。法人の管理下であるというところの具体的な要件は、欧州で何かあるか。

渋谷構成員：ISOの移行の理由については不明。御存じの方がいればご回答いただければありがたい。それから、我が国の制度にふさわしいPPに関しては、この場で御議論いただければと思う。法人の管理下というところについては特段の要求事項はないという認識だが濱口構成員から補足があればお願いしたい。

濱口構成員：FIPSからISOへの移行については、そもそもFIPSが米国の規格であり、その試験や認証の取得自体も米国の制度である一方でコモンクライテリア評価、ハードウェアの評価や EAL のレベルの高いものの評価は歴史的に欧州が主体となっているという背景から、米国の制度から欧州の制度へ移行したいというのが背景にあるのではないか。

これはあくまで個人的な意見。

PP について、QSCD の PP である EN 419 211 は委員会実施決定と呼ばれている eIDAS 規則の下位規則で具体的に参照されていて、その eIDAS 規則の要求事項と技術基準、プロテクションプロファイルとのマッピングがとれている。他方、欧州では HSM の PP として、EN 419 221 が整備されてきているものの、委員会実施決定のような下位規則がないため、EN 419 221 に関しては eIDAS との明確なリンクは与えられていない。もっとも、EN 規格として整備されているため、加盟国の国内標準として採用されるものという意味で恐らく、デファクトスタンダードになっていくものだと考えている。我が国の e シールに関する技術基準としての PP をどうするかという話だが、欧州の PP をそのまま使う案も、日本で独自の PP をつくるという案も両方とも考えられる。

最後に、法人の管理下というところに関しては具体的な要件は明確にはない。あくまで法人が自分の責任の下、自分の管理下に置くということが求められている。

新井構成員：ISO に移行しようとしている背景については承知した。FIPS に限らず幅広い選択肢を、そしてコモンクライテリアの活用においても日本独自の仕組みをという話になれば日本独自の PP を整備するという話になると考えており、これは一つの可能性としてはあると思う。

また、法人の管理下というところについては日本における電子署名法第３条と同じようなラインで書かれていると理解した。

手塚座長：HSM について、ISO 15408 系は日本でも NITE の関係で CCRA に加入しているというように国際的な相互承認の枠組みがあるが、FIPS は米国調達であるため米国のほうの基準に左右されるという見方もできる。他方、自力で基準を整備するとなると、かなりの負担増となるためこの点どう考えていくのかというのはもう少し大局的な議論になる。

濱口構成員：先ほどと意見が少し重複するが、eIDAS 規則の一部については、下位規則によって技術規則と法的要件の間の明確なひもづけというのが与えられている。例えば QSCD やトラストリストのフォーマット等一部、下位規則で、技術規則や技術基準を参照しているものがあるが認証局の基準となる EN 319 401 及び EN319 411-1、EN319 411-2、これらに関しては、下位規則実施法等で参照されていないため、これらの規格が eIDAS 規則の第 19 条及び第 24 条の TSP の要件に適合するための技術基準であるということは法律のどこにも書かれていない。ただしこの規格は EN（European Norm）規格として整備されているものであり、EU 加盟国が国内標準として採用することを義務づけられている規格であ

るため実質的にこれらの規格が使われている。

また、個人的には日本における秘密鍵の保護環境については、少なくとも秘密鍵の保護が、EU の QSCD 相当の耐タンパー環境で実施されるような環境の整備が必要だと考えている。Society5.0 や DFFT の実現に当たっては、データを自動で検証し、自動で検証されたデータの信頼性に応じて自動で処理をし、さらにそのデータが次の自動処理を生み、新たな価値を創出していくということが想定されるため、秘密鍵がきちんと保護された環境で運用されているかどうかについては検証が必須。そのため、例えば３段階の制度が出来上がったとして、レベル３において QSCD を必須とするかどうかというのは別の議論にしたとしても、QSCD を利用していることが、デジタル署名、署名値の検証において分かること、これは重要だと思う。

欧州では eIDAS 規則に基づく適格証明書であることを示す QC ステートメントと、e シール用の適格証明書であることの QC ステートメント、最後に QSCD を使っていることを示す QC ステートメントの３つがあり、証明書の識別子として格納されているため、デジタル署名値を検証することでその秘密鍵が QSCD の中にあることが分かる。日本においても QSCD を使っていることを示す識別子を入れることができる制度をつくる必要があるのではないか。

宮内座長代理：資料 10―１の９ページ目、一定の基準を満たした e シール生成装置を用いることを要件として要求するかどうかについては電子署名法等の国内の他制度とのバランス、ヨーロッパの制度とのバランスが重要になる。国内の他制度とのバランスを考えると、電子署名法や商業登記法では秘密鍵を格納する署名生成装置の規定は特に置いておらず、秘密鍵の管理は本人に任されている。実空間の世界の制度である実印等の管理が法定されていないこととパラレルで考えて、署名に用いる鍵については本人の責任で管理を行い、何か問題が生じたら本人の責任だと一般的には考えられてきた。そして、電子署名と e シールを比べたとき、意思表示を伴う電子署名は文書の真正成立の推定効を持つものも存在する一方で、発行元を示すのみである e シールがそれよりも強い効力を持つとは現時点では考えられておらず、今後も考えにくい。すなわち、一般的に見て、電子署名より効力が劣る e シールについて、電子署名よりも厳格な規定を置くというのは、全体のバランスを欠くように思う。

他方、生成装置の規定を置いているヨーロッパとの関係では、生成装置を規定する方が望ましい。仮に生成装置の規定を厳格にすると、レベ

ル３はQSCDを求め、レベル２は不要となるという整理になるがこの場合は効力にどのような違いがあるのかというところが気になっている。レベルを問わず国内法的には厳格に法定された効力はなく違いがないため、EUでの適格eシール相当として通用するかという点がメルクマールになると思うが、あくまでレベル３に特段効力を設けないという整理になると普及するかどうかについて疑問がある。

結局のところ、電子署名とeシールの両方について生成装置を求める、求めないこのどちらかが取り得る選択肢ではないか。両方に求めるということになると、現行の電子署名法からの連続性を考えると、一定の経過措置を置いて行うことになるというのも一案だが一種の規制強化になるので難しい点もある。

他方、どちらにも生成装置を用いないケースでは、ヨーロッパとの関係が問題になる。既存の国内制度と同様に秘密鍵等の管理は、ユーザーとなる本人・法人の管理の問題であり、責任であるという考え方をガイドラインの中に明記することになると思う。それに加えて、秘密鍵の管理方法として、生成装置を使う方法があるということについてもガイドラインに書く、あるいはEU等との連携を見据え国際的にも通用する効力が必要な場合には、こういうQSCDを使うことが適切という旨をガイドライン等で書いていくという方向がいいと今のところ思っている。

手塚座長：NISTのSP800-63-3のAALのところの検討を見ていると、国際的には安全性を求める方向に倒れていく流れであり、これを踏まえてレベル感を設定、レベルの高いものにはQSCDの使用を要件にする等して安全性の高い基準を設け我が国でも制度に反映する必要があると思う。QSCDを使用しないeシールについても否定せず、選択権は利用者に帰属するものの、明確にそのレベルの違い、それによる実際のシステムとしての安定性や安全性を加味し、制度の中に反映する必要がある。その上で、現行の電子署名法と見比べると難しい部分があるものの、我が国の中でのトラストサービス全体の安全性・安定性を実現するために電子署名法を直していく方向性で考え、改正に当たっては経過措置のようなものが必要かどうか等そこについて知恵を出して整理していく必要がある。

宮内座長代理：レベル感の必要性についてはおっしゃるとおりだと思うが、レベル３とレベル２を設定した場合、受け取った側にとっては両者に効力の違いがあるかどうかが問題となる。レベル３でもレベル２でも、鍵の管理等に何か問題があったときには、eシールを発行した側、eシールを生成した側の責任になるとすれば受け取る側は２でも３でもい

い。そう考えるとレベル２を使うこととレベル３を使うことによって、何が実際に違ってくるのかというところを考えないと、レベル感の差が機能せず、かつレベルの高いものが普及しないのではないか、という懸念を持っている。

手塚座長：包括的なトラストというレイヤーで考えて将来的には公的個人認証と連携するといった話になると、レベル感の話が明確に出てくる。個人認証というのはいわゆる最上級のレベル、本検討会でいうレベル３を要求しているものとなっている。そうすると電子署名法と公的個人認証法とで現状では体系が別ではあるものの、eIDAS をはじめとして、世界的には官民を分けず一本でやっている国がほとんどだということを踏まえると、現状の公的個人認証法というのはある意味特別法的にも考えられ、電子署名法を一般法として、その中の一番ハイレベルなものを規律しているというようにも見え、レベル感の概念というのは包括的なトラストの枠組みでの相互承認等を考えていくと必須になると思う。

宮内座長代理：私も公的個人認証法と電子署名法については一本化すべきだと考えるが、現状日本の電子署名法では Advanced Electronic Signature でも、文書の真正成立の推定を認める余地を認めている。その場合に、レベル３を設定することに一体何の意味があるかということは考える必要がある。この点については課題があるということを主張しており、レベル感が必要という意見に反対する趣旨ではない。

小松（文）構成員：認証局側の HSM の標準だが我が国の現状の認証局の数を考えると、国内独自の標準というのはコストがかかりすぎるため、適切ではないと思う。ISO/IEC 15408 は国際相互認証されており、PP はまさに様々な国で使用できるものであるためそれを使用すれば問題ないと考えている。

手塚座長：続いて、小木曽構成員からのコメントを代読する。欧州以外や UNCITRAL の議論をどう評価するか。単に国際といったときに欧州以外の国もあると思った、とのこと。

事務局：UNCITRAL は電子商取引であり、今回の議論のスコープからは違う気もするが、設備の基準については国際的なコモンクライテリアと米国の基準である FIPS 以外には参考となる基準はないと考えている。もしこの２つ以外にも検討の必要がある基準があれば、事務局でも検討したい。

高村参事官：補足する。小木曽構成員の欧州以外との関係や UNCITRAL の件云々という部分だが、実際どう考えていくかというのは DFFT の概念を

どこまでのリージョンで考えていくかという話と直結するため公開の場で日本政府の関係者としては回答できない問いである。仮に論点として掲げられたとしても、少なくともこの検討会の報告書に盛り込むことはしないという点は御理解いただければと思う。

新井構成員：資料 10－１の５ページについて認証局の責任の範囲外というところはもう少し突き詰めたほうがいい。電子署名法で明示的に書いてはいないものの実際に実施している調査はたくさんある。例えば、電子署名法に規定のない法人の真偽を確認するときの手順についても CP に記載し、その点を調査機関である JIPDEC に調査されている。そして、その結果を踏まえ認証局として責任を持って CP を公表している。登記されている組織等よりも細かい単位組織について、完全に認証局の責任の範囲外とされると、何のための証明書だということになる。例えば、登記された情報や印鑑などで組織の代表者である申請者が申請したものを正確に電子証明書に記載するという意味での認証局の責任であれば、そのように規定し、内容についての責任は押印や署名等で確認された代表者にあると言える。電子証明書に記録する以上、認証局の責任は問われるところであり、当該の論点としては、制度として定める部分、それ以外の認証局の独自で規定する責任部分、その中に申請者が申請したものをそのまま証明書に記載するという点も踏まえて、報告書等では書き方を留意していただきたい。

９ページについては、発行側の認証局の HSM をかなり厳格な要件にしている一方で、利用者の生成装置については要件を緩やかにして普及促進を図るというのは違和感がある。レベル３に関しては普及に資するというよりも、欧州や米国との相互承認に値する、世界的に見ても恥ずかしくないレベルであるというところを望んでいる。普及に資するレベルというところは、レベル２で、国内の申請や申告に資するものとして考えるべきではないか。

３ページ目だが、発行対象と真偽の確認対象は分けて考えた方がよいのではないか。恐らく、発行対象というのは企業内における機器や企業内組織になり、それらが利用者になる。補足だが、特にレベル３に関しては、真偽確認に用いるデータとしてはベースレジストリを軸にすべき。

事務局：責任の範囲外の記載ぶりは検討する。基本的には、発行対象の組織の代表者の申請内容を信じて尊重し、対応するということをもって認証局としての義務としては果たされていると考えている。前回構成員の皆様方からいただいた意見をまとめたつもりだが、表現ぶりについ

ては調整したい。９ページについてはコメントとしていただく。３ページ目にある発行対象については、真偽確認対象という言い方もできるとは思うが一般的にはどこの組織に対して e シール用証明書を発行しているのかといった言い方のほうが分かりやすいかと思い発行対象という言い方を使った。もちろんその対象となる組織は実在性等確認されるため真偽確認の対象ともいえると考える。

若目田構成員：企業の実態と e シールの運用がどのようにフィットするのかというところが気になっている。

この検討会の立ち上げの際には、新型コロナウイルスの感染症対策としてテレワークが求められるが、ハンコを押すために出社せざるを得ないといった問題があり、その処方箋として e シールに期待するというお話があったかと思う。企業の電子署名の運用について、例えば入札業務等に際し電子証明書を利用する場合は、社内のガバナンスポリシーに基づいたＩＣカードの利用申請、貸し出し管理、複数人チェックや専用端末による運用など非常に厳格に運用されている実情がある。出社する必要もあり、結果的に紙でやったほうが早いと思えるような部分もある。今後は、企業の運用の実態なども把握し、e シールがどうフィットするのかという点も、制度の普及の観点からもチェックをすべきでないかと思う。EU との取引等を前提にレベルの高いものを使っていくというのは理解ができるものの、実際に e シールを幅広く普及させニューノーマルに対応するといった当初の目的に則して考えることも重要と思う。

事務局：貴重なコメントとして参考にさせていただく。

山内構成員：新井構成員を補足する。電子署名法に基づく認定の対象外であっても、企業に属している人が電子証明書を使うに当たっては、当該企業の名称、役職等の属性情報も含めて電子証明書に記載されるのが通例であり、それらの属性情報も電子証明書全体の信頼性に関わってくるため、指定調査機関としての調査の対象にしている。具体的には、認証事業者が電子証明書の発行対象となる企業の実在性をどのように確認しているかを、認証業務規程の運用の確認を通じて調査している。このため、e シール用電子証明書における企業の名称や部署等についても、当該企業の言いなりになるのではなく、認証事業者がどういう規定に基づいて確認するのかのルールを定めることが重要。

次に、法律と標準は、相補完する面があって非常に重要な興味深いテーマである。私はレベル２とレベル３というものについて、技術的な標準を作っていくことを提案したい。レベル２についてしっかりと標準

を作り、レベル３については、さらに、諸外国から見ても恥ずかしくない標準を作り、それらに対応した法的効力も同時に検討していくということをお願いしたい。日本国内の実情に合わせ３段階のレベルに分け、諸外国の標準やISOのコモンクライテリアなどを引用しつつ、レベル２とレベル３についての技術標準をつくるのに合わせ、法的な効力についても検討することにより、法律と標準をバランスよく検討していただきたい。

事務局：貴重なコメントとして承る。

堅田構成員：電子署名用の電子証明書の話にはなるが、証明書の管理に関しては試行錯誤の中でやっているというのが実態。個別の業務端末を用意し、管理部門でしっかりと電子証明書の管理を行い、社内の決裁ルールや電子ワークフローのようなものに基づいて電子証明書の利用承認を取るという形でやっている。他方、このような運用だと在宅ワークだとできないという話になる。システムを導入したりID管理の徹底によりワークフローを電子化したり、外からアクセスできないような社内メールのやり取りを証跡として残した上で、シンクライアント端末等のリモートで使える端末を使って電子証明書を利用したり、会社に行かなくても決裁や電子証明書の利用ができるような形を実現できるよう検討しており、社内の整理だけで可能なものは既に実現している。今後こうしたルールが整備され、具体的なやり方として洗練されていくことが、利用できる範囲を含めた利用の拡大には不可欠であると思うが、現時点では企業側として試行錯誤している最中であるというのを補足させていただいた。

事務局：企業の中で実際に電子証明書がどう使われるのかという点は非常に重要な視点であり、ありがたい。

新井構成員：資料10－１の９ページにおけるHSMの要件や11ページにおける管理基準についても、電子署名法のものをベースにするということでいいと思う。電子署名法の記載ぶりでもHSMについてはFIPSもISOも読めるような記載ぶりになっていたと思うため、そこが含まれるような書き方になっているためそれでいいと思う。実際にどういう機器を使っていけばというのは別途議論するべきものだと思っており、制度としては今の電子署名法の記載レベルが一番いいと思う。

山内構成員：現行の電子署名法の基準はFIPS140-1のままであり、見直していく必要がある。電子署名に用いる電子証明書のHSMの話と、eシールに用いる電子証明書のHSMとで、ばらばらに基準を定めるというのではなく、デジタルトラストの枠組みの整備の中で、統一化していただき

たい。

事務局：新井構成員のコメントは HSM の要件等について賛同いただいたと認識。また、山内構成員のご指摘のとおり、電子署名法はFIPS140-1 のレベル３になっているというのは認識している。電子署名については本検討会のスコープ外となるが、将来的にデータ戦略の中で、他のトラストサービスを含めて包括的な枠組みの検討が行われるときには当然、アップデートされるべき部分だと思う。資料 10－１の９ページ目にも書いたようにタイムスタンプも国の認定制度にするにあたり、FIPS140-2 のレベル３相当以上という形にアップデートしており、e シールも同じようにレベル感を揃えるべきだとは思っている。

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