参考資料 12－１

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 11 回）

１　日　時

令和３年３月 26 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、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、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 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 11 回）事務局資料

資料 11－２　富士通株式会社提出資料（欧州調査）

資料 11－３　富士通株式会社提出資料（実証関係）

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）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 11－１について、渋谷構成員から資料 11－２、11－３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。

柴田構成員：資料 11－１の５ページと７ページにあるレベル３の e シールにおけるユーザー側の e シール生成装置に係る検討の方向性だが、e シールの電子署名との違いは秘密鍵とユーザーの関係が１対Ｎになるという点にあり、複数者の利用による利便性を確保するため、秘密鍵は複数もしくは複製可であることが望ましい。他方、複製可の場合は、管理する当事者に秘密鍵の管理が委ねられるため、秘密鍵が漏れたり盗まれたりしないような仕組みが必要。複製可であるファイルの管理の在り方について制度で規定することは個人的には不可能と考えており、複製可はレベル３には不適格ではないか。実世界の実印は唯一性があり、管理については利用者のガバナンスで対処することになっており、管理にトラブルがあった場合も不利益を被るのは利用者である。電子の場合もその点は同様だが、秘密鍵が一回漏洩すると簡単にコピーされて広範囲に流出し多大な不利益が生じる可能性があるため、安心して利用できるような制度的担保が必要なのではないか。また、容易に複製可能であることは、利用者の否認事由となってしまうことも考えられ、秘密鍵の管理については慎重な検討が必要。また機器により e シールが自動で付されるケースも想定されることも踏まえると、秘密鍵の管理を組織のガバナンスに任せることは危険だと考えている。そのため、レベル３のローカル型の e シールにおいては複製可とすることは避けた方がよい。その場合に損なわれる利便性については、一定の信頼基準をクリアしたリモート署名事業者等の第三者による管理により対応すればよく、リモート署名事業者を選択する際の信頼基準を検討することが望ましい。

手塚座長：署名生成装置の基準を置いていない現行の電子署名法に合わせるということも一つの考え方。他方、米国の NIST の SP 800-63-3 では、Identity Assurance 、 Authentication Assurance 、 Federation Assurance という３つの大きな基準があり、まとめると Identity management の概念ということになるが、要はユーザーサイドの管理のレベル感は非常に重要になっている。国際的な状況を見ていると秘密鍵の管理方法については厳格にやっていくところが見えてきているため、レベル３のユーザー側の鍵管理については重要な論点だと思っている。

高村参事官：e シールの信頼性と e シールやそれが付されているデータを発行する者の信頼性は分けて考えなければいけない。e シールはあくまで

発行者が誰なのかということを書き示すものであり、秘密鍵の管理が杜撰である発行者が出したｅシールが信用できるかどうかは、ｅシールではなく発行者の社会的信頼性が担保する問題である。

すなわち、ｅシールが付されているデータの中身が正しいかどうかは、その発行者が信頼できるかどうかに最終的には依存する。この点は技術や制度で担保する話ではなく、運用で担保し受け取った方が判断すべき話である。ID 制度にて、エンティティに ID を付与する際に信頼度を位置付けていく手段も可能性としてはあるが本検討会のスコープ外。ｅ シールが付されているという事実だけを持って発行者とされる組織から発行されたと推定するのではなく、エンティティの信頼性も考慮した上で受け手側が判断すべき点ともいえる。ｅシールが貼ってあるからノーケアで受け取っていいというものではないということを御理解いただくというほうが正しいアプローチなのではないか。

手塚座長：柴田構成員のお話や先ほどお話した内容はユーザー側の管理の仕方のお話であるものの、高村参事官のおっしゃった認証局側の話もおっしゃるとおり。

高村参事官：認証局側の話ではなく、手塚座長や柴田構成員がおっしゃったことを担保しようとすると、しっかり管理できない利用者にはレベル３の ｅ シール用電子証明書を発行しない、すなわち ｅ シール生成装置等を認定の要件として課す制度にする、又はそれを預かった以上はしっかり運用するという義務を認証局から ｅ シールの利用者に課すという話になる。しかし、その点についてはｅシールが付されたデータを受け取った方が、誰が発行者なのかという部分を見て、そのエンティティの信頼性に基づいて判断すべき事項ではないかということを申し上げている。

手塚座長：それもご認識のとおり。その際に、ユーザー側の管理が杜撰で発行者自体が特定できないという可能性が出るのではないか。そこの点についてユーザー側の管理にレベル感を持たせることで NIST SP800-6-3 は対応できている。簡単にコピーができるというデジタル世界のリスクに対応し、耐タンパ領域に格納することをレベルに応じて求めるということ。混乱を防ぐためにもユーザー側の管理についてレベル感を意識しながら、制度的担保が必要だと考えている。

高村参事官：今の話は identifier の議論が若干混ざっている。発行者がしっかりした人であるというクリアランスまで含めて ｅ シールが付与されるという前提を入れるのであれば、おっしゃるとおり。他方、本検討会で検討している ｅ シールのスコープから考えると、最終的には制度

ではなく運用で担保する話ではないか。この方向性と同じご意見なのか、それとも今後の方向性の中で、ユーザー側での厳密管理を制度の中に盛り込んで打ち出すべきという御意見のどちらか。

手塚座長：そのような概念があることをまずは認識し、論点としてあるということをしっかり認識しておくべき。

高村参事官：おっしゃるとおり。認定認証業務に係る電子署名では秘密鍵の管理をしっかりしていただきたいという旨を認証局から利用者に伝えていると思っており、これはｅシールでも求められていく。ただ、実際にどう管理されるかということ自体は利用者側の運用に任せ、最終的にデータの発行主体となる電子証明書の発行を受けた側がしっかり管理をしていくという前提の制度設計にしていくしかないのではないのかと考えている。

柴田構成員：私がお話したのは、ユーザー側で簡単にコピーができる秘密鍵をユーザー側に渡すというのは問題があるのではないか、ということ。電子署名の場合は本人に秘密鍵が渡されるため、しっかり管理されると思うが、複数の人間が同一の秘密鍵を使用することが想定されるｅシールの世界においては秘密鍵が様々なところにコピーされた上で使用されることが予想され、危険を伴うのではないか。

高村参事官：前提を確認したい。資料 11－１の７ページの１つ目のポツに「同一の秘密鍵を複数の ｅ シール生成装置に格納し」と書かせていただいているがここはあくまでも、電子証明書が複数枚発行されるというイメージでいる。事務局側としてはユーザー側で秘密鍵をコピーするということはあまり考えていなかったものの、この記述を見てユーザーサイドで秘密鍵を複製して、というご認識をお持ちになったということであれば我々と認識が異なるため、記載ぶりを修正したい。

柴田構成員：ご推察のとおり。一つの事業体に対して複数の秘密鍵と電子証明書が発行される可能性はあるものの、ユーザーサイドで秘密鍵の複製が可能となると話は別であり、その場合は複製可というのは不適格ではないか。

高村参事官：秘密鍵が IC カードに封入されているという前提に立ったときに、資料 11－１の 7 ページの①で意図していたのは、IC カードをみんなで使い回すというパターンで、１枚の ｅ シール発行装置を使い回しているため最終的な発行者が誰であるかまでは分からない。②は、中身が同じ IC カードが複数、認証事業者から渡されるパターンで、実世界で言えばショッピングモールで領収書を発行してもらうときに１階から 10 階までのサービスセンターで同じ角印を押しているといった運用

と同じように、同じ秘密鍵が入ったICカードが認証事業者から複数渡されるイメージ。そして③は、秘密鍵が異なっているICカードが１枚の申請書に対して同時に発行されるパターンで、秘密鍵自体は全部異なり、どのモジュールで認証されたのか、eシールが付されたのかをトレースできる。柴田構成員がおっしゃっているのは中身が同じICカードが複数配られるのもまずいのではないかというお話か。

柴田構成員：そのケースであればあり得るのではないか。

高村参事官：紛らわしい書きぶりで申し訳ない。もう少し厳密な記載に修正する。

濱口構成員：事務局資料11－１の５ページ目の「方向性」においてQSCD相当は要件としないとなっているため、論理データとして秘密鍵と電子証明書は配られ、現行の電子署名法における認定認証業務と同じ取扱いになるのだと想定している。実質的な問題として、ユーザー環境において秘密鍵は自由にコピーできる状況となる。

他方、QSCDを使うのであればコピーはできない、かつ耐タンパ性も保証されているため簡単には秘密鍵が漏洩しないような仕組みになる。高村参事官の先ほどの話にあった、eシールにより担保する信頼性と発行者自体の信頼性は別の話という点については賛同。そして、データの信頼性と発行者の信頼性を紐づけるものこそがeシールだと思っており、秘密鍵がどのように管理されているかによってその紐づきに強弱が出る。例えば、秘密鍵が漏洩すると真にその発行者から出たデータなのかというのは保証できなくなる。そのため、欧州のように秘密鍵の保護環境としてQSCDの規定を設け利用者以外はeシールをなしえない形にすべき、と前回意見したが現行の電子署名法の認定認証業務でQSCDを求めていないこととの関係で考えると、保護環境を要件として規定するのは難しいということと承知。これは事実上本人以外も押すことが可能であるハンコの文化でやってきた日本と、本人以外なしえない署名の文化でやってきたヨーロッパとの違いだと認識している。他方、今後のSociety5.0やData Free Flow with Trustで想定されるデータドリブンの世界を実現していくためには、データの検証者が発行者の信頼性とデータの信頼性を確かに紐づいて保証しているeシールのような制度が必要不可欠になってきておりその秘密鍵がきちんと管理されていると制度で保証されていることが非常に重要だと個人的には考えている。

宮内座長代理：ユーザーの管理についてルール上しっかりと規定すると、レベルによってeシールを生成する企業が発行者であることを否認でき

るかできないかが変わるという話になりかねない。レベル３だと否認できないものの、レベル２だと否認しやすいということを言ってはいけないのではないか。e シールの利用企業自身の過失により第三者による ｅ シールが生成されてしまった場合はレベルに関わらず本人たる利用企業の責任でなければ、受取人にとっての意義が薄れてしまい、しっかり管理するというインセンティブを落とすことにもなる。あくまでもレベル２であっても、本人の不始末で第三者に悪用されたら、本人が責任を負うということで進めなければならないと考えている。

堅田構成員：企業ガバナンスと発行者の責任を分けて考えたい。e シールが保証するデータの信頼性の基点は、データを作った人がデータを出したと言う事実であり発行者自体の信頼性等は ｅ シールでは担保できないということが前提。その上でレベル２とレベル３の ｅ シールがあったときに、企業内ではどのようなガバナンスになるか。実世界の角印を考えると、社内での一定のワークフローや決裁権限をもって押すことが可能であり、システム帳票等を対象に大量処理・一括処理をやっている。そのため、レベル２の ｅ シールについては利便性の観点から ｅ シールの認証の仕方と管理のレベルは厳しくすべきではない。他方、レベル３は契約行為に使うような丸印と同じようなものと認識しており、資料 11－１にあるような二要素認証であれば問題ないという記載が弊社内でも妥当であるとなるかどうかは若干疑問。レベル３については認証の確からしさにおいて、企業側からより高いレベルを求められるケースがあるのではないか。もっとも、弊社事業の中で関わりのある個人事業主の方々の中には二要素認証でもいい、もしくは何か別の認証方法でも問題ないという方もいるとは思う。

　複数人での共同使用については運用の問題だと思っているためここで議論する必要性はあまりないのではないか。秘密鍵の複製に関しては、システム的に付与するものや有事のバックアップを考えると認めざるを得ない、ユーザーからするとないと困るものだと考えている。実世界で考えても有事に備え、普段使用するハンコ以外にもバックアップ用のハンコを準備している。同一組織への複数の ｅ シール用電子証明書の発行は企業の実態からすると必要かと思っている。

濱口構成員：今お話しいただいた秘密鍵の複製、ハンコのバックアップについてだが、複数あるハンコは印影が同じではないと思う。その一方で秘密鍵は複製するとハンコでいう印影が全く同じになるため意味が違うのではないか。

堅田構成員：ハンコについては複数同じものを作成したとしても印影が変

わってしまうのは物理的な問題であるため、電子的な秘密鍵とは事情が異なるというお話だったが、大規模な有事が起きたときにシステムセンターが止まるということも想定しており、バックアップセンターを複数持っている会社も多くある。あるいは印刷会社で印影を管理して印刷をしていることもある。実世界ではそのようにリスクヘッジをしているものの、電子の世界ではある瞬間から突然我々が付与しているｅシールが変わってしまうことになると難しい。もちろん、違うｅシールであっても同一の e シールあるいは同じものだと確認する、システム上認識することが可能なのであれば話は別だが、複製することを考慮した仕掛けにすべき。業務や実施主体が違うものまでを１つのｅシールでカバーするということは大きな企業では想定していない。私が複製をしたいと言っているのは、同じ業務で同じようなことをやっているものの、物理的に２つの環境からやらざるを得ない場合。ユーザー側でのコピーを禁止し、それが企業の実情を考えると問題があるのではないかという問題提起である。例えば仮想 PC 等を用いた環境で RPA 等の活用を考える場合に、物理的な複製は駄目となるとシステムを作る必要が生じ、その結果 e シールの利便性を損なうということも想定される。ただ、複製を繰り返し誰がやったか分からなくなるということは企業ガバナンスとしてはあり得ないことであり、運用上担保すべき。

濱口構成員：懸念されていること自体は、秘密鍵自体を複製しなくても同じ会社に複数の電子証明書、秘密鍵を発行することで対応可能かと思う。

手塚座長：秘密鍵の管理の問題は非常に重要なファクターであり、適切な管理を運用でカバーし切れるかどうかに疑問がある。違うスキーム又は運用でカバーできているという保証があれば話は変わってくるが、我が国のｅシールにおいてはその辺りをどのように考えていくか。

山内構成員：本検討会の第２回で、JIPDEC が使用している eIDAS 規則に基づく qualified のｅシールの実例を紹介した。JIPDEC が使用しているｅシール用電子証明書と秘密鍵は厳重な USB メモリ、いわゆる QSCD の中に格納されていて、複製することはできない。そして、その USB メモリは鍵をかけたロッカーの中にしっかり入れて、一部の人しか取り出せないような形にしている。本検討会で検討しているレベル３の e シールに近いものであり、次々に押す角印のような使い方はできない。レベル３にして複製ができない形にすることは利便性の点で使いづらいものではあることを含め、実例に即しながら検討していく必要がある。

次に、資料 11－１の５ページ目に「現状の電子署名法の規制強化」という文言があるが、この表現については修正いただきたい。現行の電

子署名法に基づく特定認証業務の認定は任意のものであり、法規制ではない。「規制」という言葉は一般的には法律に基づいて国民の権利を制限したり、義務を課したりすると捉える方が多いと思うため、基本的には「規制」という言葉は使わないようにしていただき、「認定基準の強化」や「認定基準の厳格化」といった言葉に訂正いただきたい。私の持論ではあるが、法律に基づく施行規則、告示や指針などで技術基準なり認定基準を一回定めると変えることは難しい。e シールの技術基準を決めるにあたっては、e シールを発行する人、e シールを検証する人、中立の人、認証局のトラストサービスプロバイダ等の関係者を集め、標準化に向けた検討の場を作り、電子署名法の改正も含め包括的なトラストの枠組みの整備に向けて検討した方がよい。

宮内座長代理：認定認証業務は任意であるため、規制強化という言葉を使わないほうがいいという話について、それ自体はおっしゃるとおりだが、電子署名法３条の推定効の要件として QSCD を求めるということが仮にあれば EU と同等になるものの、これは規制強化といえるのではないか。

また、電子署名法第３条のような規定を e シールの制度の中に置いた方がいいという意見があったが、電子署名法第 3 条の括弧書きというのはしっかりした公開鍵暗号方式を使っている等の電子署名の方式の一般的な性質や性能を示したものであり、実際に署名者側が適正管理をすることを要件として求めている規定ではない。

全く別の話になるが、EU において電子署名や e シールはそれらが付与されているデータのことだと定義されている一方で、我が国の電子署名法では電子署名は措置と定義されている。これは民事訴訟法 228 条４項にある押印が行為であることとパラレルに電子署名法でも行為であると定義されている。この２つの違いがあるということをまずご認識いただきたい。その上で e シールについては、データと行為のどちらで整理をしたのか明確にする必要がある。この２つの違いは立会人型の電子署名が本人の電子署名に含まれるかどうかというところに関係する。e シールについても立会人型 e シールというのが許されるかどうかということが検討対象になることも想定される。

山内構成員：宮内座長代理の意見にあったように、規制強化と記載するのであれば、電子署名法第３条の推定効の要件の見直しと書いてもらったほうがいい。

事務局：コメントは承った。本検討会は我が国の e シールについてどのような要素が必要なのかというところを議論するのがメイン。電子署名法の改正や内容が適切であるかどうかは別の場での議論となる。

山内構成員：規制強化という言葉は見直していただきたい。
事務局：宮内座長代理のコメントも踏まえて規制強化と書いているが、表現は工夫する。
小田嶋構成員：e シール利用者秘密鍵の管理について、「電子署名及び認証業務に関する法律に基づく特定認証業務の認定に係る指針」第８条と同様に、認証局側もしくはリモート署名事業者は、利用者に対し重要な事項の説明を実施するよう既定すべき。指針の第８条に記載のとおり「利用者の秘密鍵に関しては十分な注意をもって管理する必要がある」説明をすることとなっているが、e シールに関してはレベル２であろうと３であろうと必要だと思っている。資料 11－1 の 12 ページにあるリモート事業者に関しては一定の基準が必要ではないかという意見、13 ページにある失効要求が可能な者としては基本的には代表者で、もしくは委任を受けた者、このあたりの方向性については賛同。同ページにあるように EU においては QC ステートメントを証明書に記載してレベル３であることを示すことができることになっている。ここについては日本独自の Object Identifier を取得できると非常に良い。日本におけるレベル３を保証する独自の Object Identifier を取得し、EU やその他の国と相互認証する際に、日本の e シールに関しては QC ステートメント確認すればレベル３だと判別できる。
伊地知構成員：資料 11－1 のリモートで付与する事業者について一定の基準が必要ということについて賛同。この点について、今後リモート e シールサービス提供事業者の要件や必要事項について検討するような御予定があればご教示いただきたい。
事務局：リモート型の e シールサービスについては構成員の皆様方からの意見も多くいただき、認証の関係に限って論点として取り上げたという認識で、細かな提供事業者の要件についてはそこまで検討していく時間的な余裕はないと思っており、それは将来的な宿題として承る。
高村参事官：リモート e シールサービス提供事業者に認定基準のようなものを入れるとすると、秘密鍵をしっかり管理する、秘密鍵を不正利用しない、この２つに尽きると思う。そのため ISMS を要求するのかどうかは別にして、ポリシーを定め、そのポリシーに基づいた運用を e シールの利用者や権限者に対し約束し、その旨が対外的に見える仕組みにするというのが基本。詳細な認定基準を新たに設けるものではないと思っており、ひとまず我々、国側の検討に委ねていただけるとありがたい。
伊地知構成員：リモート e シールサービス提供事業者が管理する e シール用の秘密鍵の安全性確保は極めて重要であるため、秘密鍵を管理する

設備の基準に関しても御検討いただきたい。

小川構成員：資料 11－２について、SAM はコモンクライテリア EAL4+という表現があるが不適切。EAL4+はレベルの説明にしかなっていなく、資料 11-１の HSM にも EAL4+との記載があり、同じ要件だと受け取られる可能性がある。そのため、EN 419 221-5 という個別のプロテクションプロファイルに基づいた認証ということを明示した方がよい。また、JT2A のリモート署名ガイドラインと LSCP 等の EU の基準が全くイコールとなると問題があると思っている、すなわち４ページ目の表にリモート署名ガイドラインのレベル１、２、３というのを並べること自体に問題があるのではないか。

濱口構成員：表形式のデータだが全くイコールという訳ではなく、同等のレベルであるということを示しているに過ぎない。今後ヨーロッパと日本で相互承認の枠組みを検討する際にも日欧で使われている技術基準やベストプラクティスの同等性が重要であり、同一である必要まではないと考えている。

また別の話になるが、e シールに先行して電子署名のリモート署名方式というのが議論されていた。リモート署名ガイドラインでは e シールはスコープ外となっているものの、e シールと電子署名において、技術的にはデジタル署名方式であるという点で全く差がない。他方、e シール固有の論点として法人内において複数の利用者が想定されることが考えられる。その際に e シールの複数の利用者において認証要素をどう管理していくかということが問題になる。

新井構成員：資料 11－１の７ページについては、ｅシールの制度として、電子署名法と同等に利用者の秘密鍵の保護環境は限定せずに規定していくことも一案である。しかし、ユーザーの秘密鍵の管理に関するルール作りは重要な論点であるため、電子署名も含めて包括的な議論が必要なのではないか。つまり、認証局からユーザーへ配付するｅシールの秘密鍵を格納する媒体やリモートに関する議論についても、リモート署名ガイドライン等を参考にしつつ、政府がしっかり関与した上で別制度として決めていく必要がある。また、電子署名法３条に記載があるような規定を設けたほうがいいと思う。

資料１１－１の１３ページの失効については、電子署名法では施行規則の第６条第 10 号に規定があり、電子委任状法では指針の第４の３の六に規定がある。電子署名法は利用者からの依頼による失効と記録事項に事実と異なるものが見つかった場合の失効の２つが規定され、電子委任状法は利用者からの依頼による失効が規定されている。ｅシ

ールについては、証明書の記載内容が重要であるため、記録事項に事実と異なるものが見つかった場合の失効も含まれる電子署名法に同等が望ましい。

最後にリモート e シールガイドラインを作る予定があるかどうか、見通しをご教示いただきたい。

事務局：リモートでの e シールを検討する上での重要な論点である認証の話については今回提示済みであり、リモート e シール特有の論点は一定程度カバーできたと認識。そのため、リモート e シールに特化したガイドラインの作成は考えていない。

小松（博）構成員：予防的統制と発見的統制の両輪で制度を考える必要がある。もし何かあったときにそれを発見してどう対応するかという発見的統制の観点から失効リストについての EU の取扱いを知っていれば教えて欲しい。失効リストには CRL 方式と OCSP 方式があり、オンラインで適時に失効しているかどうかを検証できるような仕組みが EU ではあるかどうか。失効の運用を考えると、使う人によって電子証明書も変えて、何かあったときには全部失効するのではなく、一部の電子証明書だけ失効するというやり方になるのではないか。

濱口構成員：失効リストについては、基準上は CRL あるいは OCSP のどちらかが必須となっている。当然どちらも提供することは否定されておらず、多くの認証局は CRL と OCSP 両方をサポートしているというのが実情。またどちらかが必須であるという規定はあるものの推奨されているのは OCSP である。

小松（博）構成員：原則 OCSP とする方が適切だと認識している。

柴田構成員：小松構成員の意見に賛同。法人内で使用する秘密鍵が１つの場合、失効後の業務への影響を考えて、利用者側で失効に対する躊躇が生まれる恐れがある。

渋谷構成員：失効に関しては、当事者間の申告に基づいてという報告をした。他方、認証局側も記載事項に誤りがあったり、齟齬があったりした場合には失効ができる。現在の日本における法人番号サイトでは、登記事項の変更情報についてダウンロードができるという格好になっているため、企業の実在性を確認するベースになっている登記の情報の変更情報を活用しつつ、e シールが適切に運用される必要があると思う。

事務局：リモート e シールの認証要素の管理の話については重要な論点かと思うが既にいただいた意見以外には特段の意見はないということでよろしいか。

堅田構成員：先ほどもお伝えしたがレベル３の e シールについては企業のガバナンスの観点からすると、単純な認証だけでは認められず、システム間連携による認証も求められる、すなわちよりレベルの高いことを求められる可能性がある。

宮内座長代理：資料 11－１の 12 ページに、「レベル３の e シールをリモートで付与する事業者については、一定の基準が必要か」とあり、これはおっしゃるとおりだが、当該事業者についてはレベル３の e シールしか付与してはいけないということか。

事務局：レベル２の管理レベルにある e シールの提供についても想定している。

宮内座長代理：レベル３の e シールに限定されているとも読めてしまうため記載ぶりを工夫いただきたい。

事務局：アプリケーション提供事業者等が認証要素や PIN も管理することを考えると、TSP 側で勝手に e シールをリモートで付せる可能性も出てくるため、レベル３であれば認められないが、レベル２であれば認められるという整理も考えられる。

高村参事官：補足する。リモート事業者に対して認定制度を入れるかどうかという部分について、制度の仕立て自体が最終的にどうなるのかという部分が見えていないため、お約束ができないということだけは御理解いただきたい。基本的には資料 11－1 の 17 ページにあるように、何かの認定制度を置くものがレベル３で、外形的に、技術的に動いているものはレベル２という仕切りで考えている。レベル３を運用するときにリモート e シールサービス提供事業者の基準をどうするかということは制度論としては考えやすいが、レベルを問わずしっかりしたサービス提供者ということを認定等するスキームを作れるかどうかというのは別問題であり約束はできないということをご容赦いただきたい。

山内構成員：レベル３だけの認定制度を作る場合は、それ以外のものについて、国が認めないと駄目だという形にならないような広報宣伝を心がけていただきたい。レベル２のものであっても、そのリスクに応じて十分使えるということをしっかりアピールしていただきたい。

事務局：承知した。

手塚座長：e シールを我が国の中でしっかりと使えるようにするために、レベル感を設けつつ、混乱がないように整理することで、どのレベルも我が国の中では使われるようにする。そのような視点で今後整理していくことが重要。

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