

e シールに係る検討会（第 5 回） 議事要旨

1 日時

令和 6 年 1 月 17 日（水） 15:00～17:00

2 場所

オンライン開催

3 出席者

（構成員）

手塚座長、伊地知構成員、伊藤構成員、漆畷構成員、小田嶋構成員、堅田構成員、小松構成員、境野構成員、柴田構成員、袖山構成員、中武構成員、濱口構成員、宮内構成員、山内構成員、若目田構成員

（オブザーバー）

デジタル庁、国税庁、経済産業省、一般財団法人インターネット協会、日本司法書士会連合会（欠席：法務省）

（総務省）

山内サイバーセキュリティ統括官、豊嶋大臣官房審議官（国際技術、サイバーセキュリティ担当）、小川サイバーセキュリティ統括官室参事官（総括担当）、酒井サイバーセキュリティ統括官室参事官（政策担当）、宮野サイバーセキュリティ統括官室参事官補佐

4 配付資料

資料 5 - 1 事務局説明資料

資料 5 - 2 e シールの活用が見込まれる事例に関する分析（3）

5 参考資料

参考資料 5 - 1 「e シールに係る検討会 中間取りまとめ（案）」に対して提出された意見募集結果

参考資料 5 - 2 e シールに係る検討会（第 4 回）議事要旨

6 議事要旨

1 開会

山内サイバーセキュリティ統括官より開会に当たり挨拶が行われた。

2 議題

◆議題（１）「事務局説明」について、事務局より資料５－１に基づき説明が行われた。構成員・事務局からのコメント・質疑応答は以下のとおり。

（ア）全体

柴田構成員：共通証明書ポリシーOID については今後統一的に整理がされ、活用されていくものと理解している。共通証明書ポリシーOID が統一的に整理されることにより利点があると考えている。現状の電子署名法に基づく認定制度では、誤認防止のために一つの秘密鍵から一つの証明書を出さざるを得ないが、共通証明書ポリシーOID が整備されることで同じ秘密鍵から複数の証明書を発行できる。つまり、認証局の運営側としてはコストを下げて運営することができる。このメリットを是非活かし、共通証明書ポリシーOID をいろんなところで活用していくように検討してもらえるとよい。

山内構成員：柴田構成員の発言を補足したい。パブリックコメントとして JIPDEC が提出した意見も同様のものである。「電子署名及び認証業務に関する法律」は、20 数年前に制定された法律であり、電子署名は自然人がするものであって、法人や組織が e シールを発行するという発想がなかった。昨今、欧州では eIDAS 規則に基づき、自然人が行う電子署名と法人等が生成する e シールを同様に扱うようになっている。これらの電子証明書を発行するトラストサービスが満たすべき要求事項は違う面もあるが、ほぼ共通である。ところが、「電子署名及び認証業務に関する法律」においては、認定された特定認証業務から発行された電子証明書は自然人が行う電子署名にしか使用できない。つまり、認定された特定認証業務の認証局が、同じ秘密鍵を用いて、法人向けの電子証明書、つまり e シール用電子証明書を発行したいという要望を出しても、それは認められない。ただし、電子証明書の中に共通証明書ポリシーOID を記載すると、e シール用電子証明書と自然人向けの電子署名用の電子証明書を機械的に判別できるようになる。電子署名法の主務省庁であるデジタル庁と法務省が認定していないものについて、今度は総務大臣が認定していくことで、お互いに補完できる可能性があると考えている。

手塚座長：共通証明書ポリシーOID を用いることで、法人向けの e シール用電子証明書と自然人向けの電子署名用電子証明書を機械的に判別できるため、認証局も同じ秘密鍵で複数の電子証明書を発行可能という意見と理解した。

（イ）e シールの名称

手塚座長：反対意見がないため、事務局の方向性案の通り、「e シール」という名称を正式名称として進めていく。

(ウ) e シール用電子証明書の発行対象となる組織等の範囲

宮内構成員：①個人事業主が e シールを使用することがあるのか。今後こういった場面で活用されるのかを考えていく必要はないか。②個人事業主については、なぜ電子署名ではないのか。③法的には個人と個人事業主の差はないが、税務上何か違いが出てくるのか。④例えば、書面に職業何某と記載されていたら個人ではなく職業としての事業主体というのは普通わかるので、駄目押しに e シールで確認できるようにするというイメージか。

袖山構成員：①個人事業主も法人と同じように書類の発行を行う。従来、個人事業主が発行している見積書、発注書、請求書等に押す印鑑や角印の代わりとして、法人・個人に関わらず事業を行っている主体で、e シールが活用されるだろうと理解している。②確かに個人の電子証明書は存在するが、個人として発行しているものか、事業者として発行しているものの区分がある程度必要になる。e シールと個人の電子証明書の使い方というのは一定程度分けられると理解している。③税務上は特に押印が要件になっていないので税務上という話ではないが、事業者として取引先に認識してもらう手続か、あるいは個人としての手続かの違い。④税理士業界に関していえば、たとえば税理士の電子証明書は認定認証業務により発行してもらっている。税理士が顧問先の企業や個人事業主の税務手続き等の申告手続き等を代理して行う場合に認定認証業務の電子証明書が必要となり、このような電子証明書を使うことで、税理士として代理送信がされていることが証明されている。他の業界ではそういったものが存在をしないため、e シールが活用できると理解している。

伊藤構成員：認定対象と認定対象外の区別を理解できていない。認定対象と認定対象外で別の組織識別子を使うように読み取れるが、認定対象の e シールを使う場面と認定対象外の e シールを使う場面で区別して考えないといけないのか。

事務局：基本的な違いとして、認定に係る e シール用電子証明書については告示の規定に沿って組織識別子を使用することが求められるが、認定対象外のものについては「e シールに係る指針」において推奨事項として示すことになる。

伊藤構成員：e シールの活用を提案していく側としては説明しにくいので悩ましい。

手塚座長：誤解を恐れずに言うと、今後告示ができた場合に、告示の要件を満たす e シールが認定対象で、認定を取らなかった場合は対象外、という程度の違いであると理解すればいいのではないかと。

境野構成員：e シール用電子証明書の発行対象となる組織の範囲には、日本の会社の海外拠点は対象になるのか。対象にならない場合には「日本国内」と記載すべきではないか。

事務局：基本的に、法人番号で特定をできる組織等であれば e シール用電子証明書の発行対象となることができる。

手塚座長：反対意見がないため、e シール用電子証明書の発行対象となる組織等の範囲については、事務局の方向性案の通り進めていく。

(エ) 組織等の実在性・申請意思の確認の方法

小田嶋構成員：2021 年 2 月に開催の「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）」の資料 9-3 で組織の実在性の確認方法について記載しているため参照されたい。e シール用電子証明書は用途として発行元証明であり、認証局が組織を確認して発行する観点から、類似の証明書としてサーバ証明書、特に法人の存在を確認して発行される EV SSL 証明書が挙げられる。当該証明書における組織の実在性確認は CA/ブラウザフォーラムが作成したガイドラインに従い、日本を含む全世界で実施されている。組織の実在性確認方法としては、①法的な存在確認、②物理的な存在確認、③運営的な存在確認の 3 点がある。①は商業登記で確認されるが、商業登記記載住所と実際の物理的住所に差異がある法人が相当数存在する。また、法的には存在しているが運営されていない場合もある。したがって、①だけでなく②・③を行っている。組織の実在性確認方法として少なくとも 3 種類が含まれると理解しており、引き続き検討が必要な項目ではないか。今回は保証レベル 1 と 2 があり、将来的には国際的相互承認を想定する保証レベル 3 もある。保証レベル 3 では、EU の適格証明書に相当する厳密な確認方法が求められることになる想定される。以上の点を考慮しながら適切に整理できれば良い。

手塚座長：本件については次回に結論を出したい。

(オ) 認証局/利用者の秘密鍵の管理に係る基準（認証局側）

漆畷構成員：認証局の鍵管理は電子署名法の認定認証の基準を準用するというので、FIPS 相当と記載されているが、「相当」の解釈について調査機関の判断が難しくなる点を心配している。CMVP 認証における警告に対する対応がなされているか、FIPS の認定は 5 年で失効してしまう等の判断が「相当」に当たるかという判断が難しくなっている気がする。総務大臣のタイムスタンプの認定制度では、鍵管理や HSM の基準はこれらの点をわかりやすく明瞭になるように制度が設計されているので、タイムスタンプの HSM の基準を採用した方がよいのではないか。

濱口構成員：漆畷構成員の意見はその通りだが、基準の同等性については電子署名法の認証局の秘密鍵の管理と、e シール用証明書を発行する認証局の秘密鍵の管理は同等であるべ

きと考えている。他方で、タイムスタンプの認定制度は HSM の基準に対してよりクリアに書かれていて監査も調査もしやすいという状況にある。これは電子署名法の規定が古い
ため、電子署名法の規定を改定していかなければならないという課題に根差している。電子署名法の要求事項は古い
ため、アップデートしていかななくてはいけない。

伊地知構成員：認証のステータスや警告に対する問題については実施要項に明示されているものではなく、制度を運用するにあたって解釈が定まってきた。したがって、どこにも明記されていないため、明確に公表していくことが重要ではないか。

山内構成員：FIPS140-1 のレベル 3 に関する表現は、現在の「電子署名及び認証業務に関する法律」に基づく特定認定業務の基準の中には出てこず、以前の主務省庁の 3 省庁からの局長通知、今はデジタル庁及び法務省の局長級通知に記載されている。これは「電子署名及び認証業務に関する法律に基づく指定調査機関の調査に関する方針」と言うが、その記載内容は新しくされるべきである。本検討会の直接的な対象ではないが、タイムスタンプの基準が最新だからそれに合わせるというよりは、日本全体として国が認定するものについては、日本政府としての方針を決めてもらい、基準を合わせるようにすべきである。そのような方針を出した上で、外国の規格を引用せざるを得ない場合はどの外国の規格を引用するかを決めるというように、順番をしっかりと政府の中で決めていくことが重要と考える。

漆嶋構成員：e シールの制度が既存の電子署名法の基準に倣ってしか作れないという話になると、古いやり方のまま新しい制度を始めてしまうことになるのではないかと懸念している。

手塚座長：20 年前に作ったものを参考にして、それに合わせるということではなく、全てものを最新の状態にする必要がある。e シールは新たな制度であるが、電子署名については 20 年前のままになっているため、まずそこは最新の基準に引き上げないといけない。引き上げたときにタイムスタンプを合わせて 3 つが横並びで HSM 使うとなれば、HSM の表記は基本的に同じになるとよいのではないかと考える。基準を最新にした場合に横並びになるように日本国として進めていくことがよいと考える。

事務局：ご指摘の事項は中長期的な課題も含まれる。本検討会では年度末までに結論を出すべき事項に注力して議論していきたい。

手塚座長：本件については次回に結論を出したい。

(カ) 認証局/利用者の秘密鍵の管理に係る基準（利用者側）

小松構成員：証明書を発行するという事は証明書のペアになる秘密鍵についても一定程度認定局からのポリシーが反映されるはず。最低こういうことはやるべきということに記載した方がよいのではないか。証明書ポリシーもしくは証明書ポリシーのステートメントの一環として記載すべきではないか。

漆嶋構成員：小松構成員と同じ危惧をしている。CP/CPSなどで利用者が適切に鍵を管理することを確実にしておかないといけない。実施要項等ではきちんと確認する等、完全に自由にさせるわけにはいかない。

宮内構成員：秘密鍵の管理が不十分で問題が起こったときはその管理者の責任ということをはっきりとすれば、その責任のもと利用者側で好きなようにやればよいのではないか。何か良くないことが起こったときに秘密鍵の管理が不十分だった場合には、秘密鍵の管理者が責任を負うべきことであると明確にし、さらに CP/CPS に記載するとよい。

小田嶋構成員：事務局資料の抜粋の（１）に記載されているように、現行の電子署名法に基づく認定認証業務と同様に e シール認証局に関しても、重要事項の説明で利用者に対し「利用者の秘密鍵は重要なもので厳重に管理される必要があり、紛失・盗難などがあつた場合には失効しなくてはならない」等の案内義務を設けられる必要がある。

堅田構成員：企業での使われ方を想定した場合、e シールの信頼性の強度が実態としてどこに依存するかは重要なポイントである。例えば、e シールの発行に至るまでの企業側での業務プロセスの確からしさや e シールの管理レベルの方が今論議している e シールにおけるルールに関するところよりも影響が大きいケースもある。e シールに関する厳しいルールを作るだけでなく、書類などの重要度に応じて適切な管理をすべきということをはっきりとすることが、e シールの普及にとって重要なポイントであると考えている。加えて、（２）に書かれているが、プロセスの中でしっかり管理できていることが e シールを見たらかわかるようにすることにも価値がある。生成装置を使ったケースなど、厳格な管理と運用が徹底されているとわかる状態にしてほしい。こうした点も含め、全体として、整理いただいている方向性に違和感はない。

手塚座長：秘密鍵をどのように管理しているかをきめ細かくガイドしておいたほうがよいのではないか。最終的にどこまで基準として書き上げるのか、事務局においては基準を書くかも含めて整理されたい。

(キ) e シールを大量に行う際の処理

堅田構成員：まとめて e シールを付与するときに他の電子文書が紛れることがないことをサービス提供事業者側で担保するとは具体的にどういうことを想定しているのか。

事務局：「ただし、一括で e シールを行う際には、(中略) 他の電子文書が紛れ込むことがないことを e シールサービス提供事業者側で担保する必要がある。」は、確認的な意味合いとして記載したものである。

堅田構成員：大量データを作るときに、たとえばサービスの API など一度に呼び 10 個の文書に付与できるようなイメージを持っていた。特に大量データを作るときに、e シールサービス提供事業者側に改めて別の措置を求めることはないという理解で合っているか。

事務局：その理解である。

堅田構成員：論点④(2)で生成装置を使ったときにきちんとした管理がなされているのかわかるようにしておくようにと書かれているが、複数の文書に付与するときも同じようなことが考えられる。複数の文書に e シールを付与する場合、どういうプロセスか、どういう装置なのかなどをわかるような記載とすべく検討してほしい。

伊藤構成員：「一括」という表現になっているが、100 個の文書に対して一つの e シールをするわけではなく、一つずつ e シールを付与していく理解でいいか。

事務局：その理解である。

濱口構成員：一つのドキュメントに一つの e シールを大量に打っていくという認識である。方向性案には賛成している。複数の対象データに一括で e シールを打てた方が便利である。ただ、その詳細を検討していく上で、どのようにそれを許すのかというところに注意が必要である。特にこれが問題になるのはリモートで e シールを付す場合であり、10 個のドキュメントをあらかじめリモート e シール生成事業者にアップロードして、それに対して e シールを付すという指示の仕方、あるいは秘密鍵を一定期間活性化して使える状態にしておき、その後、対象文書を送って e シールを付す等、様々ありリスクと便利さを天秤にかけて基準を検討していく必要がある。

手塚座長：反対意見がないため、複数の対象データに e シールを一括で付与するという事務局の方向性案の通りに進めていく。

(ク) 利用者における e シール用電子証明書の失効要求

宮内構成員：電子署名法施行規則の第六条において、一定の場合の認証局からの失効について規定されており、これと同様に CP/CPS に委ねるまでもなく、認証局から失効してよいと指針に記述していいのではないか。

小松構成員：内容には異存ないが、CP/CPS に今後どのようなことを規定しないといけないのかについて今後検討が必要と考える。今までの議論の中で CP/CPS に書くべきものは多分にあったため、整理していくべきと考える。

事務局：制度の詳細については次年度に検討することとなるが、年度末までに結論を出すべき部分を整理の上、次回に再度議論させて頂きたい。

手塚座長：CPS だけでなく電子署名法の施行規則第六条のように、下位規則に書くという方法もあるのではないか。今回の結論としては、失効要求できる者は e シール用電子証明書の発行を要求できる者に限定するという点は反対意見がないため、事務局の方向性案の通りに進めていく。他方、認証局からの執行要求については次回再度議論することとしたい。

(ケ) 認定制度の在り方に係る論点

伊地知構成員：指定調査機関について、適合性評価については ISO/IEC 17065 などに基づく認定を受けた適合性評価機関が進めるべきと意見が上がっているところと思う。そういう中で、今回指定調査機関という仕組みを選択されたのがどういう考えに基づくものなのか教えてほしい。特に国際相互承認を見据えたときにどうなのか。たとえば、EU の経済連携協定などでは適合性評価の結果の受け入れを促進する広範な仕組みが存在することが記述されている。その中には、政府による適合性評価機関の指定も含まれている。指定調査機関という仕組みで国際相互承認が可能であると考えているのか、それとも国際相互承認を想定した上位レベルとなった段階で、認定の仕組みに移行する必要があると認識しているのか。このあたりを教えてほしい。

事務局：国際相互認証を見据えたという点については中長期的な検討が必要な課題と理解しており、そこは前提としていない。電子署名やタイムスタンプに係る認定制度を参考に、指定調査機関を設けることを検討している。

伊地知構成員：他の分野の国際相互承認で、EU の認定を受けた適合性評価機関と日本の指定調査機関が同等に扱われたケースがあるのか知っていれば教えて欲しい。

事務局：事例は承知していない。

堅田構成員：認定の有効期限を2年にすることに関して、利用者としてはやはり一定期間のサービスの継続性がないと使いづらいところがある。例えば大量にeシールを発行する場合、システム対応も想定され、5年や7年などシステム構築期間を含めると結構長い間サービスとの連携が必要になるため、2年でサービスが終了してしまうと利用者に影響が大きい。そのあたりを具体的にどう配慮していくべきか、検討してほしい。また、元々発行していた事業者が認定取り消しをされた場合、eシールの効力はどうなるのか。その効果が遡及してなくなるのか、あるいはその当時確認したことを利用者側で保管しておけばよいとするのかについても、明確にしていくべきではないか。

袖山構成員：認定の有効期間2年という点について異論はない。認定タイムスタンプの有効期間は10年間だが、タイムスタンプに倣うとeシールの認定期間2年というのは認定の有効期間が2年として捉えているのか、あるいは現在電子署名の認証局で運用されている電子証明書のように電子証明書自体の有効期間は認証局ごとに設定できるのか、どちらの認識か。

事務局：認定に係る認証業務の有効期間についての議論である。

山内構成員：「電子署名及び認証業務に関する法律」では、認定は1年ごとの更新となっている。国の認定は非常に重いものであり、基本的に全体のスキームの整合性をとるのであれば「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の有効期間と同じように1年にするのが素直ではないか。また、一たび更新を2年ごととしてしまうと、1年ごとにすることは困難であろう。国の中で別々の有効期間があることがよいかどうかは、十分にデジタル庁や法務省と相談して決めてもらいたい。

境野構成員：指定調査機関としてはどのような企業が候補として想定されるのか。

事務局：参考として、電子署名ではJIPDEC、タイムスタンプでは日本データ通信協会が指定調査機関となっている。

手塚座長：本件については次回に結論を出したい。

◆議題（2）「関係者ヒアリング」について株式会社三菱総合研究所小川氏より資料5-2に基づき説明が行われた。構成員・事務局からのコメント・質疑応答は以下のとおり。

宮内構成員：本事例は興味深い。リモート e シールで e シールの実行を指示できる人は、一人なのか大勢いるのか。

三菱総合研究所 小川氏：具体的にはここで書いてあるサポート作業を行う作業員が実際にアップロードするため、様々な方に e シールを付与する権限がある。

宮内構成員：そういう人たちが複数いて、どの人がやったのかというはちゃんとログでわかる仕組みになっているという理解でよいか。

三菱総合研究所 小川氏：その理解である。

宮内構成員：リモート e シールサーバ側から見たときに鍵認可は 1 種類なのか。それとも人によって違うのか。セキュリティとしてはきちんとしてほしいと考えている。

三菱総合研究所 小川氏：確認を取りたい。

伊地知構成員：ご紹介の事例では、署名鍵の生成はリモート e シール生成サービス事業者が行い、e シール用電子証明書発行要求もそこから送信されている。それを受けて、認証局が e シール用電子証明書を発行している。この認証局が総務大臣認定を取った事業者である場合、リモート e シール生成事業者についての制度はないが、この状態で総務大臣認定の e シールを生成できると理解してよいか。

三菱総合研究所 小川氏：リモート e シール自体で細かく定義しないといけない事項はあり、新しい規則は当然今後検討することになる。リモート e シールを含めないで証明書を付与するという点では、認証局が総務大臣の認定を取得して事業を行っていくことになる。

伊地知構成員：4 月以降に検討予定の実施要項等で定める規定によるところがあるかもしれないが、リモート e シール生成サービスに係る制度ができる前にリモート環境で総務大臣認定の e シールを付与できるとの理解でよいか。

事務局：電子署名との並びもあるため、リモート e シールサービス事業者に係る論点についてはリモート署名の議論も参考に検討を進めていく必要があるが、制度としてリモート e シールを排除するものではないと考えている。

3 閉会

事務局から、次回の日程について説明。

次回日程：2月5日（月）15時～17時

以上