参考資料３－１

トラストサービス検討ワーキンググループ（第２回）　議事要旨

１　日　時

平成 31 年２月 15 日（金）16:00～18:00

２　場　所

総務省８階　第１特別会議室

３　出席者

（構成員）手塚主査、新井構成員、小笠原構成員、小川構成員、繁戸構成員、柴田構成員、袖山構成員、谷構成員、西山構成員、古屋構成員、宮崎構成員

（ヒアリング対象者）アドビシステムズ株式会社今西氏

（オブザーバー）吉田内閣官房情報通信技術総合戦略室参事官、篠原法務省法務専門官、布山経済産業省情報プロジェクト室係長、木村経済産業省サイバーセキュリティ課課長補佐、大澤一般財団法人日本情報経済社会推進協会センター長（代理）

（総務省）竹内サイバーセキュリティ統括官、泉大臣官房審議官、木村参事官（総括担当）、赤阪参事官（政策担当）、豊重サイバーセキュリティ統括官室参事官補佐、小笠原大臣官房企画課長、山路データ通信課長、小高情報システム管理室長、飯倉情報通信政策課調査官

４　配付資料

資料２－１　小川構成員提出資料

資料２－２　アドビシステムズ提出資料

参考資料２－１　トラストサービス検討ワーキンググループ（第１回）議事要旨

５　議事要旨

（１）開　会

（２）議　題

①　前回会合の振り返り

事務局から参考資料２－１に基づき、前回会合の振り返りが行われた。

②　構成員・関係者ヒアリング

小川構成員から資料２－１について、今西氏から資料２－２について説明が行われた。

③　意見交換

構成員・関係者ヒアリングの後、意見交換が行われた。主な意見等は次のとおり。

西山構成員：一番重要な点は、リモート署名で署名をした場合に電子署名法第３条の推定効が働くかという点。電子契約を推進するためにも、リモート署名で生成された電子契約書等について、法律的な裏付けにより電子署名法第３条の推定効が働くという建て付けをつくることが非常に重要。電子署名法第３条における「本人による電子署名（符号及び物件を適正に管理することにより、本人だけが行うことができることとなるものに限る。）」というところが最大のポイント。EU では Sole Control（署名者本人のみが鍵を管理すること）のレベル２の場合は本人が署名をしたに違いないとされている。日本でもそうした基準を固める作業が必要。

小川構成員：リモート署名に不安があることで、その利用が進まないという問題意識から、事業者を集めて日本トラストテクノロジー協議会（JT2A）を立ち上げ、リモート署名について検討を行っているところ。

柴田構成員：日本では長期署名という言い方があるが、電子署名を長期保存するためのタイムスタンプという論点も重要。EU においては、eIDAS 規則において、Advanced Electronic Signature が規定されているところ。AdES ではタイムスタンプが必要。日本では、電子署名法にタイムスタンプは一切規定されていない。リモート署名について議論する際はタイムスタンプも含めた整理が必要。

宮崎構成員：電子署名を用いる意義を考えれば、文書が誰によって作られたかを、単にその文書を受け取ったときに確認できるだけではなく、電子契約書について何年後かに係争になった際にも証拠として通用するようにすべき。EU では、タイムスタンプを打って必要な期間だけ有効性を保てる仕組みを含めて電子署名として定義しているが、日本ではタイムスタンプについて法的な根拠がない。法的にタイムスタンプを定義して、タイムスタンプを使って長期間有効性が保てる電子署名の仕組みを整備することが必要。

古屋構成員：クラウド環境の進展を踏まえ、リモート署名は非常に重要な論点。リモート署名のシステムを実装するに当たっては、本人確認について、保証レベルの考え方を踏まえることが非常に重要。保証レベルによる、満たすべき要件のレベル分けについての検討状況はどのようなものか。

小川構成員：米国では、NIST の SP800-63-3 において、重要な取引については電子署名を推奨する旨の規定があるのみ。

EU では、eIDAS 規則において、Sole Control のレベルによりレベル分けがされ、レベル２を満たすものは適格電子署名となる。

日本では、Sole Control のレベル２相当を要求すると、高額なハードウェア・セキュリティ・モジュールが必要となり、リモート署名の普及を阻害す

る懸念があり、どのようなリモート署名がリーズナブルに市場で受け入れられるかという観点も含めて、JT2A において検討しているところ。

古屋構成員：個々のシステムでセキュリティを確保しようとすると、要件も膨らみ、費用も大きくなるため、何らかの基準が必要。難しい問題であるが、引き続き検討いただきたい。

谷構成員：リモート署名のシステムを運用するためには、サーバサイドやクライアントサイドであっても、アプリケーションモジュールやハードウェアモジュールだけではなく、それらが搭載されるプラットフォームの安全性も考慮する必要があると考えられるところ、その点についてはどのような検討がなされているか。

小川構成員：EU においては、ETSI の資料によれば、モバイルを用いた署名について、クライアント環境については検討中と思われる。

　米国においても、NIST から発行されているバーチャルマシンに関するプロテクションプロファイルについて、近年は新規発行やリバイスがされておらず、検討中と思われる。

手塚主査：プラットフォームのところについては一応安全という前提で、まずはアプリケーションモジュールやハードウェアモジュールの領域だけを検討しているということか。

小川構成員：おそらく、決めるべき事が非常に多いので、コアの部分から検討の範囲を広げているのではないかと思われる。

新井構成員：電子証明書の発行の際、IC カードが用いられることがあり、本人が持っていることと、PIN を打って本人を確実に確認できることという２要素をもって安全とみなされているが、電子署名法においては、電子証明書が IC カードにないといけないという規定はない。リモート署名も含め、本人確認の際に、安全性をどのように確認すべきかは重要な論点。

　また、小川構成員の資料にあるとおり、登録から発行までについては電子署名法に規定があるが、その後の運用や管理については全く規定が無いため、その点を明確化した上で、リモート署名についても議論すべき。

　小川構成員の資料に、「署名レベルの定義がない」とあり、「署名レベル」は Advanced Certificate と Qualified Certificate を指しているのではないかと思われるが、日本でも電子署名法上、特定認証業務と認定認証業務が定められており、それぞれ完全に Advanced Certificate と Qualified Certificate に相当するわけではないものの、日本でもある程度レベル分けはされている。EU における Qualified Certificate は、ヨーロッパ国内での基準を定めており、日本においても、国際的に通用する基準を作るのであれば Qualified Certificate を目標とすることになるが、日本国内に限って言えば、電子署名法だけで十分な確認はできているため、Qualified Certificate を目指す意義を明確化し、議論を進めていくことが重要。

手塚主査：小川構成員の資料において、「リモート署名において重要な鍵ペアの安全な管理・利用シーンについては、規定がない。」という表現があるが、印鑑の例で言えば、登録した印鑑の運用・管理についての規定は存在しておらず、その理屈がそのまま電子署名法でも展開されている。しかし、電子の世界では、2048 ビットの鍵をトークンにどう入れ、運用管理していくかが非常に重要な課題になっており、例えば IC カードやマイナンバーカード等で鍵を管理するといったことも必要。その課題がリモート署名という論点で顕在化しており、検討していく必要がある。

海外では、鍵の運用管理を場合分けして考えており、例えば NIST の SP800-63 ではハードウェアで管理していれば一番レベルが高く、ソフトウェアレベルの管理はレベルが下がるといったように、保証レベルに差異を設けている。

西山構成員：先ほどの新井構成員の発言に関して、小川構成員の資料でいうところの「署名レベル」は、Qualified Certificate ではなく Qualified Electronic Signature を指している。Qualified Electronic Signature は、eIDAS 規則において①適格電子証明書（Qualified Certificate）、②IC カードやハードウェア・セキュリティ・モジュールのような適格署名生成装置、③ETSI の標準で定義された先進電子署名（Advanced Electronic Signature）の３点から構成されると定義されており、適格電子署名は手書きの署名と同等な法的な有効性を持つとされるなど、日本の電子署名法とは差異があるため、Qualified Certificate と Qualified Electronic Signature の混同には留意すべき。

小笠原構成員：リモート署名には、どこからでも署名をすることができ、各企業のワークスタイルの変革につながるという大きなメリットも存在する。従来の IC カードによる電子証明書の管理では実現できない出張中の決済や契約といったユースケースもリモート署名では実現できるため、リモート署名を使いたいという企業も多く存在するのではないか。

一方で、古屋構成員からも発言があったとおり、どこまでシステムを作り込めば顧客に安全性を納得してもらえるか、現状では明確な基準がないため、基準を作成することで、リモート署名の普及につながると考える。

袖山構成員：税理士は代理送信といって、eTAX を通じて納税者たるクライアントの申請を代行できるが、代行のためには、税理士会から IC カードの発行を受け、eTAX のシステムに認定認証事業者の発行している電子証明書を登録し、利用者識別番号を入力し、PIN を入力するという、非常に面倒な作業が必要であり、このような電子証明書の使いにくさが、eTAX の普及が進まない一因と考えている。

金融機関においては、インターネットバンキングの普及が進んでいるところ、インターネットバンキングでは入金伝票や出金伝票が存在せず、ベンダーが残している取引のログだけが取引の証明になっているという課題があ

る。取引の安全性を保証するためには、何らかの証明書の発行や、認証について法的な整備をするといった対策が必要。

　また、本ワーキンググループでの検討にあたっては、データの真正性、取引の安全性、保存領域の安全性の混同に留意すべき。

繁戸構成員：建築士が図面に署名をし、15 年間保管することが建築士法で定められているが、それを建築業として行うためには建築士事務所の事務所登録を行い、所属する建築士の資格を管理する必要がある。

　図面への署名の電子化を進めていくために、電子署名を用いることができることは承知しているが、電子署名を有効に 15 年間保管することを法律でいかに認めるか、事務所という法人格が資格をいかに電子的に管理できるようにするか、双方の検討が必要。また、これらをリモートでも行えるようにしなければ電子化は進まない。建築業界は働き方改革や労働時間削減を強く求められている業界でもあり、安心して電子化を進めていき、労働時間の短縮を図っていきたい。

西山構成員：繁戸構成員の発言に補足をすると、建築士の電子署名がされた設計図書は電子的に保存ができるということが、建築士法第 20 条と e 文書法制定に伴って制定された国交省令（国土交通省の所管する法令に係る民間事業者等が行う書面の保存等における情報通信の技術の利用に関する法律施行規則）で定められているところ。

　建築図書の電子的な作成においても、リモート署名を利用している事例もあるほか、建築確認申請という行政手続では、指定確認検査機関がリモート署名のサービスを用意し、建築士の電子署名にタイムスタンプを付与して長期署名の形で保存しているという実態もあり、非常に利用しやすいモデルと聞いている。

小笠原構成員：繁戸構成員から、建築業では文書を何十年という単位の長期間保存する必要があるという話があった。何十年もシステムを維持することは、事業継続性の観点も含め、大きな課題であるところ、トラストリストという形で、過去に作成された文書の真正性も保証できるようになるとよい。

　また、日本産のシステムを海外に展開することを考えると、EU のような明確な基準がある国のシステムとの同等性を評価ができる基準があれば、システムを作る際により安価に短期間で作ることができると考えられる。

新井構成員：電子署名と、アドビシステムズが提供する電子サインの違いは何か。

今西氏：電子署名は、電子署名法でいう特定認証業務に対応した形の技術を使ったものあり、PKI の電子証明書を使って署名データを作成するもの。電子サインは、安全性を確保されたクラウドサービスのストレージで、データやデータへのアクセスの記録等を管理するもの。

新井構成員：電子サインと電子署名を単体で比較すると、安全性は若干電子署名の方が上回るが、電子サインはウェブやモバイルアプリケーションを利用で

き便利である一方で、電子署名は HSM（ハードウェア・セキュリティ・モジュール）を用いる必要があり、利便性には劣るという認識でよいか。

今西氏：御認識のとおり。

新井構成員： CSC（クラウドシグネチャーコンソーシアム）の規格では、電子署名と電子サインが両立されているが、両立のポイントは何か。

今西氏：CSC は様々な事業者が集まっているので、電子サインの部分はアドビが本業としてサービスの枠を用意して機能強化を行っていく一方で、リモート署名における鍵の管理をはじめとするワークフローは、リモート署名の事業者に任せる仕組みにし、電子サインと電子署名をつなげるための基準となる規格を決めている。

新井構成員：リモート署名の議論も、CSC の規格を考慮すれば、よりよい議論ができるか。

今西氏：そう考えている。

新井構成員：今西氏の資料 19 ページは、小川構成員の資料 21 ページとどのように対応するか。

今西氏：小川構成員の資料との対応関係は深くは考慮していない。リモート署名の詳しい仕組みは承知していないが、CSC としては、リモート署名から渡されるデータを API ベースで受取り、電子サインのサービスで使う仕組みを考えている。

柴田構成員：今西氏のプレゼンテーションの中で重要な点は、電子署名の検証の可否。アドビの商品には、AATL や EUTL といったトラストリストに掲載されている証明書が証明書ストアのリストに載っており、それを基に検証ができる。日本でもトラストリストを作成し、それをマシンリーダブルで検証できる仕掛けを構築していく必要がある。

今西氏：EU のトラストリストのようなものが日本でできれば、アドビのリストに載せ、検証できるようにすることは可能。

手塚主査：トラストリストのルール化について、法律レベルで行うのか、CSC のような自主基準レベルで行うのか、我が国としても検討していくべき。

今西氏の資料 19 ページに関して、電子サインとリモート署名の間では、ハッシュ値のみをやりとりして、ハッシュ値の運用管理に鍵を用いた暗号化や署名をしているという理解でよいか。

今西氏：然り。リモート署名では、文書全体を送って署名することもできるかと思うが、電子サインでは、利用者から預かった文書そのものを外に出すことは望ましくないという考えから、ハッシュ値のみをやりとりしている。

小川構成員：サーバサイニングアプリケーションであれば、対象データからハッシュ値を算出して、適切にモジュールに送り、署名値が来たらフォーマッティングしてドキュメントすることができるが、電子サインはサーバサイニングアプリケーションを用いないため、どのように検証できるか、JT2A で検討

しているところ。

④　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