参考資料１５－１

トラストサービス検討ワーキンググループ（第 14 回）議事要旨

１　日　時

令和元年 11 月８日（金）14:00～15:45

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、宮内主査代理、新井構成員、小笠原構成員、小川構成員、楠構成員、繁戸構成員、柴田構成員、渋谷構成員、袖山構成員、中村構成員、西山構成員

（ヒアリング対象者）セキュア IoT プラットフォーム協議会豊島氏、株式会社三菱総合研究所安江氏、柴崎氏

（オブザーバー）中田内閣官房情報通信技術総合戦略室企画官、藤田法務省参事官室局付、中村法務省法務専門官、伊東経済産業省情報プロジェクト室室長補佐、中野経済産業省サイバーセキュリティ課専門職、山内一般財団法人日本情報経済社会推進協会常務理事

（総務省）竹内サイバーセキュリティ統括官、二宮大臣官房審議官、岡崎大臣官房審議官、赤阪参事官（政策担当）、高岡サイバーセキュリティ統括官室参事官補佐、横澤田サイバーセキュリティ統括官室参事官補佐、小高情報システム管理室長

４　配付資料

資料１４－１　セキュア IoT プラットフォーム協議会提出資料
資料１４－２　リモート署名の制度化に向けた論点について
資料１４－３　トラストサービス検討ワーキンググループ最終報告書骨子（案）について
資料１４－４　三菱総合研究所提出資料（非公開）※1
参考資料１４－１　トラストサービス検討ワーキンググループ（第 13 回）議事要旨（未定稿）※2
※１、２　資料１４－４、参考資料１４－１はメインテーブルのみの参考配付

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１４－１に基づき、前回会合の振り返りが行われた。

② モノの認証について

豊島氏から資料１４－１について説明が行われた。

③ 意見交換

モノの認証についての説明後、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：資料１４－１の５ページについて、最終的な IoT の利活用のイメージをもう少し説明いただきたい。IoT 機器を埋め込んだデバイスについて、デバイス内もしくはデバイス間で通信をする場合のデータの信頼性を公開鍵暗号基盤（PKI）ベースで検証できるようにしたいという認識でよろしいか。

豊島氏：然り。PKI で認証することで、正しい人へサービスを提供して、正しい人からサービスの対価をいただくというという仕組みができあがると考えている。

西山構成員：PKI で認証するのであれば、どこかでデータの真正性を検証するプロセスが走るのではないか。通信でトラストアンカーを確認できる仕組みが必須になると考えているが、そのあたりはどのようにイメージしているか。

豊島氏：当初は PKI ベースでサーバ上の電子証明書とデバイス側に埋め込んだ電子証明書だけで全て賄おうとしていた。しかし、装置が組み上がったときにその部品１つ１つに証明書を埋め込むことは現実的ではないことがわかった。したがって、各部品には電子証明書ではなく、外からは取り出せない“鍵”を埋め込み、各部品の“鍵”の組合せをサーバで保持し、当該組合せに対して電子証明書を発行し、その電子証明書をデバイス側、資料１４－１でいう 14 ページの充電ステーションのコントローラに渡して検証を行うという取組を行っている。そのため、電子証明書ベースの認証と、暗号鍵での認証という二段階の認証方式が必要だと考えている。

西山構成員：資料１４－１の 10 ページに記載の課題「大量の IoT 機器の管理」の項目に「CRL（証明書執行リスト）、OCSP（Online Certificate Status Protocol）の大量問い合わせの課題」とあるが、サイバートラストとしては大量の IoT 機器を PKI で検証する場合の対策として二段階認証の取組をしている理解でよろしいか。

豊島氏：証明書ベースでは、10 万個レベルの数の検証が可能であることは実績として確認がとれているが、実際に車等の例では、末端のデバイスを含め 1000 万個レベルのオーダーで部品が存在するため、現行のプロセスでは性能が足りないと考えており、将来的には我々の認証局の性能を改善することで対応しようとしている。

今回示している１個１個の部品の検証に関しては、それぞれを認証局で認

証するのではなく、証明書ベースの認証と、暗号鍵での認証という２段階の認証方式を検討している。

西山構成員：分散型で検証ができるような仕組みをデザインしているということか。

豊島氏：然り。

宮内主査代理：例えば認証局は、確かに本人に証明書を出しているということに関して責任を持っている。責任の所在がどこにあるのかに関して証明書を受け取った人間が明確にわかることが重要であるが、モノの認証においては鍵を確かに埋め込んだということに関して、責任の所在はどこにあるのか。また、証明書を受け取った人間はその責任の所在が明確にわかるようになっているのか。

豊島氏：メーカーの責任で鍵を埋め込むことになる。もちろん我々からは、外から鍵を取り出せないように、いわゆるルート・オブ・トラストに相当する技術を使った鍵を埋め込む仕組み自体は提供するが、実際にデバイスの中にどのように鍵が埋め込まれているかというところまでは、確認できない。

宮内主査代理：すなわち、最終的に鍵を埋め込む部分でミスがあった場合、メーカーの責任になるということか。

豊島氏：然り。

宮内主査代理：そのような責任関係は利用者から見てもわかるようになっているのか。

豊島氏：まだなっていない。

宮内主査代理：誰が何の責任をとっているかを利用者に対して明示することができなければ、トラストサービスとして十分とは言えないのではないか。是非ご検討いただきたい。

豊島氏：メーカーとも話をして、責任の所在を明確にするようにする。

手塚主査：本日の豊島氏の話は基準作りの話ではなく、技術検証をしているレイヤーの話。モノの認証をトラストサービスとして機能させるためには、今の基準作りの議論を経て、制度化して運用しなければならない。

　モノの認証に関しては考えなければならないことが非常に多いということが認識できたのではないか。

新井構成員：資料１４－１の 10 ページの普及の課題の法的根拠に記載の「電子署名法における「認定認証業務」相当の認定制度の検討」についてはどのようなイメージをお持ちか。また、PKI の処理が重いという話もあったが、ID ベース暗号やブロックチェーンといったものがある中で、認証の仕組みとして PKI を選択した理由を教えていただきたい。

豊島氏：１点目に関しては、私からは回答できないため改めて回答させていただきたい。２点目に関しては、PKI の優れている点として、暗号化通信、認証、否認防止、改ざん防止などの多様なケースで用いることができること、電子証明書に情報を付加できること、証明書に期限を付けられることがあげ

られると考えている。特に証明書に期限を設けられる点は非常に大きなファクターである。ただし、PKI と先ほど紹介した暗号鍵の方法を適材適所で使い分ける必要がある。

渋谷構成員：総務省の戦略的情報通信研究開発推進事業（SCOPE）の取組に関して、IoT 機器の信頼性を確保するためにチップを埋め込むという話があったが、新規に製造される IoT 機器、あるいは既存の機器であっても改造可能な機器に関してはチップを搭載することで対応が可能だと理解したが、その他のものについてはどのように対応することを検討しているのか。

また、IoT 機器は国内だけでなく海外も含めて相互に流通すると認識している。セキュア IoT プラットフォーム協議会では、国際的な枠組みに関して、2020 年以降どのような計画があるのか。

豊島氏：チップを搭載できない機器に対する認証やセキュリティの確保については、現時点では２つの方法が考えられる。１つは通信のプロセスの１つ手前にゲートウェイに相当する機械を設置し、ゲートウェイまでのセキュリティを確保することである。もう１つは OS のプロセスの中にソフト的にチップを埋め込むことである。

海外の基準への対応に関しては、当協議会で海外の基準について勉強会を実施している。また、基準が業界によって異なるという現状があるため、各業界のメンバーを集い、それぞれの業界のスタンダードについても勉強しているところである。

④　リモート署名の制度化に向けた論点について

事務局から資料１４－２について説明が行われた。

⑤　意見交換

リモート署名の制度化に向けた論点についての説明後、意見交換が行われた。主な意見等は次のとおり。

新井構成員：リモート署名は認証局がリモート署名事業者に署名鍵を直接渡すことになるが、電子署名法施行規則第６条の利用者に鍵をまず渡さなければならないという規定と整合がとれないのではないか。そのようなことを踏まえると、資料１４－２の３ページ目の最後に記載があるように、電子署名法第３条のみ検討するのではなく、電子署名法施行規則第６条に関する見直しやモニタリングも必要なのではないか。

事務局：ご指摘の通り、電子署名法施行規則には認証局から利用者に鍵を届ける方法しか記載されていない。我々としても、リモート署名を電子署名法に位置づけるためには、リモート署名事業者に対する鍵の受渡し手法を、電子署名法施行規則に記載すべきと考えており、このようなことも含めて認定基準

を検討していくべきだと考えている。

西山構成員：補足だが、現状認定認証業務でリモート署名が使えないのかというとそんなことはない。利用者自らがリモート署名事業者のリモート署名サーバに鍵をアップロードするという方法で可能である。ただし、認証局とリモート署名事業者が直接鍵をやり取りするモデルは施行規則上認められていないため、その部分については検討が必要。

新井構成員：資料１４－２の３ページの「運用状況のモニタリング」のイメージはどのようなものを考えているのか。

事務局：ご指摘のモニタリングとは、日本トラストテクノロジー協議会（JT2A）のガイドラインを満たすとされるリモート署名事業者を使ったリモート署名が、既に電子署名法に基づいてサービスが提供されているローカル署名と比較して十分に安全なものなのかどうか等をモニターするイメージである。

新井構成員：認定認証業務以外のサービスのモニタリングを行うということはどういうことか。

事務局：資料１４－２の２ページのリモート署名型を使った場合における認証業務は認定の対象にならないと考えており、リモート署名事業者を介する形で認定認証業務を行うことを可能とするには、省令の改正等が必要になると考えている。そのような改正を行うために、最終的にガイドラインができ、世の中である程度リモート署名が普及し、リモート署名が一定程度どのようなものか見えてきた段階で、電子署名法の中でどういった対応ができるのか考えていきたい。

渋谷構成員：資料１４－２の１ページの EU におけるリモート署名関連の標準を参照しながら、とあるが、米国における状況等は考慮しないという認識でよろしいか。

小川構成員：当該ガイドラインでは、多要素認証の使用を定めており、米国における NIST（米国国立標準技術研究所）の定める SP800-63-３という基準にも適応していると考えている。

宮内主査代理：資料１４－２の３ページの２番目の■の「民間の自主的な仕組みを設けることが有用」という点について、資料１４－３にある国による認定と国による基準の提示の比較表のようなものをリモート署名の資料にも記載することが必要ではないか。

事務局：タイムスタンプやｅシールについては国の関与が必要であるということで、国の関与の手法を比較する表を作成し議論いただいたが、リモート署名に関しては、電子署名法研究会以降、ひとまず民間で基準を作ることを前提に議論が行われてきたと理解しており、それを前提に適合性評価の仕組みを作るとなると、その主体は民間であると考えたため、このような案としている。

宮内主査代理：とりあえず国は関与しない方向性で進めていくのか。目標地点は

どこなのか。ひとまず現状の民間の基準を前提にした議論で大きな問題はないのでその方向で進めていくということだとしても、リモート署名について公的な関与の必要性に関する議論をまったく記載しないというのは、他のトラストサービスと比較してバランスを失するので、何らか記載すべきである

⑥　トラストサービス検討ワーキンググループ最終報告書骨子（案）について
事務局から資料１４－３について説明が行われた。

⑦　意見交換
トラストサービス検討ワーキンググループ最終報告書骨子（案）についての説明後、意見交換が行われた。主な意見等は次のとおり。

宮内主査代理：資料の構成について２つ提案をしたい。まず１つ目は資料１４－３に２ページの目次に「総論」「検討の視点」を記載し、９ページの第二部の冒頭部分で「総論」として第一部の総括を行い、それに基づいて、トラストサービスの法制度の必要性、日本が目指すべき方向性を述べ、トラストサービスの枠組みについてのイメージを示し、その共有を図るべきである。また、「検討の視点」として、第一部の総括から留意点が導出されると思われることから、その関係を論理的に記載いただきたい。そしてこの総括と方向性に基づいてタイムスタンプ他のサービスを深掘りする、というロジックを丁寧に記載いただきたい。
２つ目は第二部の各論の検討にあたっての留意点、特に横断的な要素①～④について、例えば②一定の要件を満たしたTSPのリストを、機械可読な形で公表することについて、どのような留意をしたのかを明記すべきであると考える。このようなことに鑑みて資料を編集していただきたい。
事務局：ご意見を踏まえて検討する。
西山構成員：資料１４－３の９ページの「検討にあたっての留意点」について留意した結果、各論での検討に反映されない点があるのであれば、別の場所にその点に関する方向性について記載すべきではないか。
事務局：ご意見を踏まえて検討する。

⑧　トラストサービスの活用・普及による経済効果等について
安江氏から資料１４－４について説明が行われた。

⑨　意見交換
トラストサービスの活用・普及による経済効果等についての説明後、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：ブラウザに格納された信頼ある第三者認証機関のリストというものがあるが、これは米国の企業が行っているため、分類としては米国と言うことで資料１４－４の 11 ページに記載してもいいのではないか。

　また、「Adobe による独自のリスト」と記載があるが、Adobe 独自に判断しているわけではなく、WebTrust の認定を受けた認証事業者や EU のトラストリストに掲載されている認証事業者が、Adobe のリストに掲載されている。機械可読可能な形でトラストアンカーを開示することが重要であるということが資料１４－３にも記載されていたが、Adobe が自身の製品の中でそれを実現している。そういう意味では Adobe の事例は参考にできるのではないか。

柴田構成員：資料１４－４の６ページ目に関して、経済効果ではなく提供者側の市場の大きさということでしかなく、トラストサービスがあることで、デジタル化が推移することによる経済効果という視点のほうが適切ではないか。その辺を考慮してまとめていただきたい。

安江氏：その点については理解している。必ずしも経済効果ではないとは言い切れないが、本ワーキンググループで経済効果として位置づけないことにするということに関して異論はない。

手塚主査：各構成員は実際にビジネスを行っているかと思うので、感覚的にこのようなオーダーでいいのか、肌感覚としてどのような認識をお持ちかお聞かせ願いたい。

袖山構成員：電子化に係る相談を大企業から受けることが多いが、ユーザ側での効果は、まず電子化をするかどうか、というところが大きな分岐点になる。資料１４－４の３ページに書かれているのは、文書情報の取扱いに関して電子化することで直接的なコストを削減する、あるいは、間接コストを削減することで生産性を向上させることであるが、大企業の電子化の目的と、中小企業の電子化の目的は異なるのではないか。一般的に言われている電子化は、保管コストや業務効率化がメリットになるが、大企業の場合は、内部統制や監査、あるいはコンプライアンスが最終的な電子化の目的になる。

　そういう意味では、コストメリットよりも、後者のような内容をメリットとしてどう捉えるかどうかを分析したほうがいいのではないか。他方、中小企業の電子化は、業務効率化や保管コスト削減がメリットになるため、電子化の際にトラストサービスが必要になる理由を明確にし、関連サービスが提供されるときにトラストサービスのユーザも増えるようレポートを作成いただきたい。

新井構成員：資料１４－４の６ページについて、電子署名等が増えれば電子契約や電子申請等の様々な場面で活用されることが期待されるため、肌感覚としてはトラストサービス自体の市場規模よりも関連市場の市場規模の方が伸びるのではないかと感じているが如何。

安江氏：関連市場の定義（範囲）が非常に難しく、今回はかなり限定的に捉えて資料１４－４を作成している。みなさんの感覚や意見も踏まえて修正していきたい。

中村構成員：紙やはんこでやっていることを電子化した場合にどのようになるのか、という点のみに終始している点が気になる。現行の直接業務以外に、トラストサービスの導入を標準化し、制度の裏付けを作り、普及させていくことで、どういった価値の創出に繋がっていくのかという観点をもう少し盛り込んでいただきたい。

安江氏：定量的には難しいため、定性的な記載を検討する。

⑩　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