参考資料４－１

タイムスタンプ認定制度に関する検討会（第３回）

１　日　時

令和２年５月29日（金）16：00～17：30

２　場　所

WEB会議による開催

３　出席者

（構成員）東條座長、柿崎座長代理、伊地知構成員、岩間構成員、上原構成員、梅本構成員、小木曽構成員、小田嶋構成員、西山構成員、宮崎構成員、山内構成員、吉田構成員、若目田構成員

（オブザーバー）朝山法務省民事局商事課課長補佐、山崎財務省主税局税制第一課課長補佐、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）竹内サイバーセキュリティ統括官、岡崎大臣官房審議官、二宮サイバーセキュリティ統括官室審議官、大森サイバーセキュリティ統括官室参事官(総括担当)、赤阪サイバーセキュリティ統括官室参事官(政策担当)、近藤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３－１　タイムスタンプ認定制度に関する検討会（第３回）事務局資料

資料３－２　日本データ通信協会提出資料

参考資料３－１　タイムスタンプ認定制度に関する検討会（第２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

②タイムスタンプ認定制度に係る認定の基準について

資料３－１について事務局から、資料３－２について伊地知構成員から説明があった。

③意見交換

主な意見は以下の通り。

上原構成員：時刻トレーサビリティの証明方法の中でエビデンスの中に専門家による鑑識報告等とあった。ここで指す専門家とは、内部専門家と外部専門家のどちらなのか、その専門家による証明があれば、ある程度第三者性を担保した確認と言えるのかについて教えていただきたい。

伊地知構成員：TSA が自ら立証する方式が確立しているわけではないが、ここで示す専門家は、第三者であることが望ましいと考えている。

上原構成員：社内だが影響を受けない者がやるという意味で第三者性が望まれるということは大変ありがたい。

岩間構成員：TAA は日本独自でガラパゴスな存在であるという指摘があった。しかし、ITU-R の勧告でタイムスタンプの時刻監査には TAA による第三者監査が必要と規定され、JIS や ISO にも同様の規定を作っている。例えば ISO/IEC 10814 パート４でタイムスタンプの時刻配信については時刻監査機関（TAA）をいれるとなっており、それらの規定を日本の機関は遵守しているという認識。

宮崎構成員：資料３－２の６ページについて質問。時刻同期の精度の部分で TAA の方が精度が低いと記載がある。当局がしっかり監査するため、TAA の方が精度が高くなりそうな認識を持っていたがその認識は間違っているか。また、同ページの費用の比較イメージについて、費用感も本当にそうかというところが気になっている。TSA が自ら立証するなら設備や補助的な仕組みが必要になるはず。これほど差がつくのかというところが疑問。内訳を詳しく伺いたい。

伊地知構成員：TAA 自体は原子時計を置いているため、極めて高い精度で同期をしている。しかし、TAA から TSA のところについては NTP を応用したプロトコルによる同期をしているため、同期精度が高いわけではない。一方で、TSA が自ら立証する方式については GPS などを活用したタイムサーバーの時刻同期の精度をイメージしている。これはマイクロ秒程度の誤差に抑えられるため非常に高精度になると思う。同ページの費用についてだが、ここについては細かい数字は御紹介しにくい。TAA の費用はそれぞれの契約によるため、それが幾らとは開示できない。それから TSA が自ら立証する方式についても、一つの事例から算出した費用で概算している。ケース・バイ・ケースで、100 のところが 90 ぐらいにしかならない事業者も、100 のところが 5 になるような事業者も

存在し得る。

柿崎座長代理：GPS や GNSS を時刻源とした時刻同期について意見を述べたい。GPS や GNSS を用いる場合、その信号自体を改ざんされることで誤った時間を受け取ってしまう可能性がある。そのため、GPS や GNSS のみを時刻源として用いている方式が例えば中国では１社、EU では２社あると報告が上がっているが、これは将来的に問題が起きるのではないか。そのため、時刻源として少なくとも UTC(NICT)は基準とするとして、それ以外にも GPS や GNSS などの時刻ソースを用いるのは妨げないという方式のほうがいいと思う。

伊地知構成員：GPS などの信号の場合は妨害電波などもあるため、複数の時刻源を参照するのが基本だと考えている。NTP の標準の考え方でも３つ以上参照するのがベストとなっていると思う。次回以降の議論に向けて、その辺りを具体化していきたい。それから、日本でやる場合においては、例えば光テレホン JJY とか、こういった NICT の提供しているサービスを用いて、UTC(NICT)に確実に同期できる方法を選択するのがベストだと認識。

東條座長：GPS、GNSS というのは時間が狂う可能性があるので、公開 NTP のほう、こちらを主に時刻源とするべきだという御意見と伺ったが、如何。

柿崎座長代理：GPS や GNSS を時刻ソースとしても、公開 NTP として使われる場合はあると思う。現状ではそれほど問題は起きていないはず。しかし、これからタイムスタンプビジネスが盛んになったときに、誤った時刻を無理やり TSA に押させて時刻を狂わせるということが考えられるため、GPS や GNSS のような改ざんができるものをソースにするのは危ないのではないかという懸念がある。少なくとも１つは NICT を基準にするべきではないか。

事務局：NICT にプラスして GPS を時刻源として用いるとか、改ざんにさらされないような工夫が必要と承知。次回以降の議論の際に参考にさせていただきたい。

東條座長：事務局資料の「検討に当たっての主な観点」の一つである、既存の制度からのシームレスな移行の部分について、今回の方向性として、TSA が自ら立証する方式を仮に加えることになった場合、方式を追加するだけなので既存の事業者への影響は、特に問題ないということでよろしいか。

事務局：次回、TSA 事業者の方にコメントいただくような場を設けることを検討している。

東條座長：続いて、設備面の基準について意見交換をお願いしたい。

宮崎構成員：まず、FIPS140-2 のレベル３認証相当以上という説明がある。ここの「相当」の意味だが、これは何もFIPS140-2 レベル３が要求している要件を認証評価機関が全部チェックするわけではない。例えば、安全性強化のため、認証を取った製品のファームウエアのアップデートがあり、改めて認証を取り直さなければいけない場合がある。その時に、認証に期間がかかることで、認証から外れるケースがある。そういった場合でも要求要件については、安全性が劣っているわけではなく、むしろよくなっているということで、認証している製品とみなしましょうという意味で、相当という用語を使っていると認識。

もう一点はセキュリティ要件について。コモンクライテリア（以下、「CC」という。）側のセキュリティ要件として、数値的な基準を書いていないが、ヨーロッパでは保証レベルはEAL４以上ということを規定している。それを取得するためには、形式的な評価以外に、実際に中程度以上の能力を持った攻撃者が攻撃をして、安全性を分析して確かめるというようなステップも必要になっている。このようにしてFIPS の側と同等以上の安全性の保証ができるような仕組みになっている。

柿崎座長代理：HSM において CC を採用することについて異論はない。一つ注意しなければいけないのは、CC はあくまで評価についてやっているものであって、HSM の内部で使われている暗号モジュールについてどうだということはCC では議論されないということ。結局、暗号モジュールについてはFIPS の 140-2 レベル３などが採用されていると思われるので、CC で認証を取れている HSM だから安全かというと、また別の問題も出てくるのではないか。

宮崎構成員：民生ではEAL レベル４というのは最も高いと言われている。低いものでは形式的な評価しかしないが、高いレベルになると実際のアタック試験、分析をすることになっている。例えばEAL4 プラスとでもいえるものなどを視野に入れれば、その辺りも保証できてくる。

東條座長：CC でも暗号モジュールはある程度カバーされているというということでよろしいか。

宮崎構成員：そう認識している。ヨーロッパでは既にそうした運用をしている。

柿崎座長代理：すると、EAL をどうするのかというところが議論の焦点になると思う。

宮崎構成員：FIPS140-2 レベル３相当の製品は高コストとあるが、これはCC でも同じ。ただ、今回検討している対象はデジタル署名、電子署名をベースとしたトラストサービスということで、秘密鍵を守るというのは

本質的なこと。ここにある程度コストがかかるというのは妥当だと考える。コスト面で比較して、こちらが高いから、こちらが安いからということにはなかなかならないと思う。

東條座長：CC は 30 か国以上が参加する国際協定に基づいているものだということだが、中国はこれに加盟しているか。

伊地知構成員：中国は加盟していないと認識している。

東條座長：中国はどのような基準に準拠しているか。

伊地知構成員：中国の HSM については確認が取れていない。HSM を使用しているというのはヒアリングなどで話が入っている。

東條座長：それでは、最後の審査プロセスの効率化についての意見交換をお願いしたい。

小田嶋構成員：資料３－２で 17 ページの最後のセンテンスについて。こちらのセンテンス自体に異論はない。例えば電子署名法の認定で同じ確認をしているもので、既に証があればエビデンスを省略するということ自体は特に問題ないと思う。

ただし、運用や体制のところで工夫が必要。まず、申請側のほうはドキュメント提出の際に省略の対象となるものが電子署名法の法令や指定調査機関の作成している調査表のどの部分に該当するかを明示することが必要ではないか。受け取る側の認証機関のところでも工夫が必要。申請のあった事業者が電子署名法の認定を受けていることを確認しなければいけない。タイムスタンプの認証機関が電子署名法の指定調査機関と同一であれば、突き合わせをして確認ができる。しかし、認証機関が電子署名法の指定調査機関と同一でないとすると、どのように確認するかということが必要になる。

例えば、電子署名法の認定があるかどうかに関しては公表されているため、これは自明だと思う。他方、詳細な内容、例えば設備がどの場所、どの建物、どの区画にあるか、さらにその中の設備がどうかというのは実際に見ないと分からないこともある。かつどのような運用をしているかといったところに関しては、確認が必要であるため、最終的には、タイムスタンプを認証する機関と電子署名法の指定調査機関で、双方のノウハウなどを共有するということが必要。

事務局：具体的なやり方については今後検討させていただきたい。

山内構成員：２つコメント。まず一つは、今日のアジェンダの立て方について。トラストサービスプロバイダー（以下、「TSP」という。）であるタイムスタンプ局が行うトラストサービス自体の適合性の評価に関する基準、その中には設備面の基準とか組織体制の基準が入ってくると思

うが、その話と、具体的な審査をするやり方の審査プロセスの効率化の話が一緒の資料の中にあり、かつ一緒の時間帯に議論しているのは違和感がある。審査プロセスの効率化の話は、トラストサービス自身の満たすべき要求事項を決めた後で検討すべきではないか。

もう一つの意見は、サービス自体を評価する際には、サービスを行っている TSP 自体についてもその体制がしっかりしているかどうかということの基準をつくり、評価する必要があるのではないか。ヨーロッパの ETSI の場合だと、ETSI の EN の 319 の 401 で TSP の一般ポリシー要件は決まっていて、その上に積み重ねていく仕組みになっている。大局的なところから御議論いただきたい。

伊地知構成員：非常に重要な観点だと思う。当然、EU のように主体に対する基準があって、それからそれぞれのサービスに関する要件が決められている。こういう形に持っていきたいとは思っている。ただ、昨年以来の検討で浮き彫りになった論点を念頭に置いて作成したことから、効率化の観点のものが交ざっているというのは御指摘の通り。できる範囲で対応していくのがよいと認識。

山内構成員：様々なトラストサービスがこれから出現する。認証局あるいは e シール、その他のトラストサービスがあるわけだが、ベーシックなところについて TSP はこういう一般的なポリシー要件が必要だというものをつくっておくことが重要。縦割りの制度が日本の中で乱立することはあまり適当ではないと考えている。

事務局：設備面及び認定の基準の話と認定の中身が決まった後のプロセスの話は、切り分けが必要ではないかという御指摘だが、今後踏まえて検討したい。また、事業者に求められるべき要件、前回、例えば財務的な安定性が必要ではないかとか、これは吉田構成員からも頂いている。そちらも今後の検討で反映できるところは考慮してまいりたい。

宮崎構成員：認証についてもモジュール化をして、ベースのところと特別なところを分けて統一的にやっていくべき。ISMS の認証機関とトラストサービスの認証の機関というのは、ずれているところもあるため、統一を取っていかなくてはいけない。

東條座長：有効期間についてもコメントをお願いしたい。

宮崎構成員：有効期間が一つの例で、認証によって有効期間がばらばらである。それだとあまり効率がよくならない。

西山構成員：今後様々な TSP が出てくるわけだが、共通ポリシーのようなものをしっかりつくって、それをベースにやっていくアプローチが認定のスキームとして必要だろう。細かいところはトラストサービス推進

フォーラムのようなところで準備して検討したい。

小田嶋構成員：様々なTSPが出てくるときに、全て異なるようなポリシーというのは受け入れづらいと思っている。せっかく今、タイムスタンプ認定制度に関する検討会と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をやっている。共通のポリシーを１つ固めるといったことはとても重要だと思う。

吉田構成員：TSPは非常に大事なトラストアンカーであるため、事業としてどうなのかということをきちんとやらないと、コンシューマーは安心して使えないと思う。もう一つ確認したいのが、やはり海外とのインターオペラビリティーという意味で、同じレベルになっているのかというところ。

伊地知構成員：インターオペラビリティーについて。タイムスタンプそのものの規格などは標準に基づいたものを使っているため、流通性は高いと思う。TAAの利用に関しても実はISOで決まっているが、世界各国が採用していない状況である。そのような中でコストに反映するところも考慮し、どのように制度をつくっていくのかが非常に難しい議論になると思う。一方で、国際相互承認という観点で考えると、適合性評価機関や認定機関のスキームについても合わせていかないと最終的には相互承認ができないのではないかというところは非常に大きな観点。ただ、そこについては、タイムスタンプの制度化の中だけで議論するとなるとスコープが少し違うのではないかと認識。

若目田構成員：情報信託機能の認定スキームの検討においても、情報銀行そのものの認定基準の検討と、認定団体の要件の検討を明確に分けて議論し、すっきりと整理ができた。

西山構成員：国際的なインターオペラビリティーという観点については幾つかの要素が絡んでくる。一つは、技術的に例えば、EUの認定タイムスタンプと同等な技術基準のマッピングをやっていくというやり方で、相互に有効性を認めようというやり方。もう一つは、法的同等性を確認するというプロセスがある。これはおそらく政府間交渉というような形になる。ただ、いずれにしても、技術的同等性をしっかり訴求しないといけない。正確には去年の検討会から出ている４つの観点がある。そのうちの１番目が法的同等性、２番目がスーパーバイズと監査制度、３番目が技術的同等性、４番目がトラスト・リプレゼンタティブと言っているトラストリスト。技術的な同等性を確認するマッピングはしっかりやっていかなくてはいけない。

事務局：国際相互運用について御発言があった。法的に同等とみなせるかと

いうのはガバメントでも議論しているところ。これも昨年来、10 月とか 12 月とか折に触れて EU 側が日本に来る機会等を捉えて議論している。EU 側がその法的な同等性をどこまで求めるのかというのは、関係機関によって捉え方も若干違っているところもある。これは引き続き EU 側と折衝する機会、ワークショップ等で検討していきたい。

東條座長：それでは、TAA の扱いについては、TAA が保証する方式に加えて、TSA が自ら立証する方式も加えてはどうかという方向性が示された。具体的に我が国が採用する方法については次回引き続いて議論をしていただきたい。

続いて設備面の基準だが、別の方式、基準に基づく認証についても、活用することで調達先の裾野を広げていくことが適当であるという方向性が確認された。

最後に審査プロセスの効率化について。ここはプロバイダー全体の共通のクライテリアを定めるべきだというようなことも含めて、もう少し議論の整理が必要になるが、全体の方向性としては、そういったレベル感の違いを整理した上で、審査プロセスの効率化についても取り組んでいくということ。

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