参考資料９－２

タイムスタンプ認定制度に関する検討会（第８回）

１　日　時

令和２年 11 月 13 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、小田嶋構成員、小松構成員、西山構成員、宮崎構成員、山内構成員、吉田構成員

（プレゼンター）株式会社野村総合研究所山本氏

（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８－１　株式会社野村総合研究所提出資料

資料８－２　タイムスタンプ認定制度に関する検討会取りまとめ骨子（案）

参考資料８－１　タイムスタンプ認定制度に関する検討会（第７回）議事要旨

５　議事要旨

（１）開　会

（２）議　題

①タイムスタンプの海外動向に関する調査の結果について

資料８－１について株式会社野村総合研究所から説明があった。

②意見交換

主な意見等は次のとおり。

西山構成員：日本との差異についていくつか確認したい。１点目は、タイムスタンプ局が用いるTSA公開鍵証明書について、EUの場合は適格性が付与さ

れた公開鍵証明書が推奨されているが、日本の場合はその部分の規定がないという部分に差異がある。２点目は、TSA公開鍵証明書の有効期間について、EUの場合は３年であるが、日本の場合は11年と３か月程度であり、中国の場合は30年であるという部分に差異がある。また米国を中心とした民間団体であるCAブラウザフォーラムで検討されている、コードサイニングに用いるタイムスタンプ用のTSA公開鍵証明書の有効期間は確か135か月であるので、日米・EU・中でTSA公開鍵証明書の有効期間にかなり差があるという感覚を持っている。３点目は、監査の頻度について、EUの場合は、サーベイランス監査を含めて、適合性評価機関による毎年の現地監査があるが、日本の場合は現行の日本データ通信協会の制度において調査機関による調査は２年に１回であるという部分に差異がある。大きな項目での差異は前述の３点であると理解したが、間違いがないか。また、その他に大きな項目で認識しておくべき差異はあるか。

山本氏：今示された３つの観点についてのそれぞれの差異は、調査から得られた結果として間違いないので、認識は合っている。独自の方法で運用されている米中との違いを除けば大きな差異は他にはない。

柿崎構成員：中国の裁判所が採用しているタイムスタンプのほとんどがUTSAのタイムスタンプであるという話があったが、他の国のタイムスタンプが裁判所に提出されているという記録やそれが証拠として採用されなかったという記録はあるか。日本やEUで発行されたタイムスタンプが裁判所に証拠として提出されたときに、法的に適切に採用されるのかどうかという点が重要であるので気になっている。

山本氏：そこまで深く情報を追い切れていない。今の点については再度確認したい。

岩間構成員：資料８－１の７ページについて、UTC(k)との差異が±１秒を上回る場合は、タイムスタンプトークンの発行を停止するという話があり、これは日本の場合も同じであるが、うるう秒のときにも、±１秒以上ずれる可能性があるが、そのようなときにもタイムスタンプトークンの発行を停止するのか。

山本氏：今の点については調査項目に含まれていない。総務省と相談しながら、追加の調査ができるかどうか検討したい。

岩間構成員：今の点は本筋ではないので、追加の調査を行うかどうかは総務省の判断でよい。

小松構成員：資料８－１の14ページについて、サーベイランス監査と更新時の監査を分けて、２年間の間に交互に実施することが説明されているが、更新時の監査は合理的保証の監査なのか、限定的保証の監査なのか。またサ

ーベイランス監査は限定的保証の監査なのか、それともそれ以外の監査という形で調査業務や合意された手続きといったものなのか。監査手続のレベル感が分かれば、教えてほしい。

山本氏：サーベイランス監査は、認定時の監査と更新時の監査から何か大きな変更点が生じていないかどうかを確認するもので項目の50%程度を見ているが、認定時の監査と更新時の監査はすべての項目について監査するものというレベル感しか分かっていない。

吉田構成員：中国と米国ではEUのような国家のタイムスタンプ認定制度がないということに対してどのような評価がなされているか。中国と米国では、制度がないことによって、何か弊害や問題が生じているのか、そして我が国ではどうかという議論をしなくてもよいのか。

山本氏：中国は、中国ならではの特殊事情に基づいて、タイムスタンプを運用しているため、日本での制度検討にあたって参考になるようなところがほとんどないという認識を持っている。米国については、政府機関が関与する訳ではなく、基本的には民間ベースでタイムスタンプが運用されており、日本で検討している制度とは方向感が違うと認識している。

事務局：米国では民間中心にタイムスタンプが運用されているという想定はしていたが、主要な国をカバーするという意味から米中を見るということで調査していただいた。調査の結果米国はプライベート中心で、EUは加盟国一括で制度を定めているということが改めて分かり、それらを参考にすることで、日本としてどのような制度にするのかを考えてきた。制度がないということも含め、今回調べたことは参考になる情報であると考えている。

吉田構成員：制度がないという事実だけでなく、それをどう評価するか、ということが重要。今回の制度はEUと同じ制度設計になってくる。EUは参考にしやすいが、制度がないということに対して、今後の国際協調も含めて、どのように対応していくのかを考える必要がある。

宮崎構成員：資料８－１の18ページについて、ドイツの場合、サービス運用中に保管義務のあるアーカイブのログ等は、サービスの引継ぎ先となるタイムスタンプ局が見つからなければ、監督機関が保管することになると記載されているが、このような方法を採っている国がドイツだけなのか、他の国にもあるか。

山本氏：総務省と相談しながら、追加の調査ができるかどうか検討したい。

東條座長：廃止の場合の手続は重要であるので、ぜひ追加の調査について検討してほしい。

山内構成員：資料８－１の５ページについて、EUの仕組みにおいては、eIDAS規則に基づいて適合性評価機関が監査を行い、その結果に基づいて、国家

監督機関が適格というステータスを付与していると記載されているが、実際には、ETSIの標準に対して、タイムスタンプのサービスに関する適合性を評価し、合格したことを示す認証証書（サーティフィケート）という紙の文書を、トラストサービスプロバイダーに対して出している。その部分は認証活動であるということを追記してほしい。

山本氏：資料８－１の５ページに、ご指摘の内容を追記する。

③タイムスタンプ認定制度に関する検討会取りまとめ骨子（案）について

資料８－２について事務局から説明があった。

④意見交換

主な意見等は次のとおり。

小田嶋構成員：資料８－２の17ページの電子署名とタイムスタンプの認証機関の間で双方のノウハウを共有する必要があるというところは守秘義務や、事業者側と監査を行う側の関係性などを踏まえて、上手く調整できればよい。資料８－２の20ページや23ページについて、事業体全体の要件は前提に、タイムスタンプという１つのセグメントでも相応程度の要件が必要であると考えている。会社全体として問題無く運営しているかもしれないが、タイムスタンプ事業は赤字になっている場合、経営判断として事業を存続しない可能性があるためであり、そういうことも含めて、捉えてもらいたい。資料８－２の28ページについて、各社の認定の時期がずれているため、2022年度以降に認定を取得する事業者は2021年度にトラストリストに掲載されないことになるのではないか。国の認定を取得した事業者だけがトラストリストに掲載されるのか、ゆくゆくは認定を取得する事業者も認定を取得することを見越して、トラストリストに掲載されるのか。そのような部分も含めて、検討が必要であると考えている。今回答は得られないと思うが、論点として記載してほしい。

事務局：あくまでも認定制度が始まって認定を取得したタイミングでトラストリストに載るということが自然な形ではないかと考えているので、認定を取得した事業者がトラストリストに順次載っていくという理解である。

高村参事官：今の点について１点補足したい。おそらく併存期間については、トラストリストに関するものと、制度上、正しいものとして認められるかという２つの観点があると考えている。総務省として認定したという形で告示するものについては、総務省が認定しないとトラストリストには載せられない。そういう意味では、トラストリストに載るのは総務省が認定し

たものだけになる。その一方で効果の面を考えると、27ページに記載されている諸所の認定タイムスタンプの位置づけを持っているものがある。これらは改正していく際に、経過措置という形で、いつまでの期間においては、このようにみなすという経過措置規定を置くという方法もある。この移行期間においては、日本データ通信協会の制度で認定したものも、総務省の新たな制度で認定したものも同等に扱われるという形で整理することも検討したい。

小田嶋構成員：今の補足で納得した。翌年度に認定を取得する事業者にとって、不利益になってはいけないと考えている。

上原構成員：国際通用性の問題について確認したい。米国に認定制度がないことを考えると、我が国で国による認定制度を整備しても、国家間での相互承認はできないのではないか。また、制度がない現状では両国で発行されたタイムスタンプをお互いに受け入れるにあたって、ハードルはないということか。国が認定していないならば、信頼性は低いと考えるということで今回議論してきたが、逆に言うと、同じ考え方であれば、米国のタイムスタンプの信頼性は低いという認識になってしまうのか。

高村参事官：ご指摘はごもっともであると思う。米国との関係を考えると、米国はタイムスタンプの制度自体は持っていないので、いわゆる民民の世界でタイムスタンプを使う場合、双方の合意が基になる。その一方で、両者の間に紛争が発生した場合、何を使うという合意があったということを土台に論争が行われるので、国の制度がなくても問題ないということになっている。他方、政府機関が何を受け入れるようにするのかという問題もある。そのときに日本側に制度があれば、日本側の事業者は基本的にはその制度で運用していることの裏書でもって、その正当性について、国際標準に則っているのと同等の形で主張を行うことで、当該技術についての詳細な説明の立証責任から逃れることができる。制度を持っていない米国に対しても、国の認定制度に基づいて運用されているタイムスタンプサービスを使っているということが、強い証明力を持つことになる。米国が特殊なのは、NIST標準と呼ばれる、国がその技術を取り扱う場合の標準規格を別途作成して運用している場合が多いということ。タイムスタンプの場合、この標準規格に対応していないと受け取らないという標準規格がまだ存在していないのでよいが、それが出来た場合には、日本のものも認めてほしいという主張の根拠になるので、国の制度で運用しておくことは利点があると思う。

上原構成員：中国の特殊事情も似たような部分があるのではないかと思う。理解が深まった。

吉田構成員：今回の取りまとめ骨子（案）は、非常によくまとまっている。認定の単位が、日本データ通信協会の制度に比べて大きく舵を切ったところであるが、この部分の考え方について教えてほしい。EUと同じ形にするのか、我が国独自で考えていくのか。

事務局：EUと同じ単位になると認識している。現行においても、１社が１サービスを提供する場合もあれば、１社が複数のサービスを提供する場合もある。提供しているサービスごとに認定をし、それぞれに紐づくTSA公開鍵証明書が存在するという理解である。

吉田構成員：EUとは少なくとも整合性があるということで理解した。

西山構成員：資料８－２の28ページについて、認定の範囲を確認したい。各事業者において提供されているサービスは、認定を受けるときにおそらく鍵を新しく作って、それに基づいてサービスが提供されている。例えば、Aというタイムスタンプサービスがあって、それが認定されると、認定後に新たに生成されたタイムスタンプについてのみ国の認定が及ぶのか、あるいは、Aというタイムスタンプサービスは、業務としては同じ名前になっているので、認定以前の鍵で付与されたタイムスタンプで、認定時にも有効であるタイムスタンプに対しても、国の認定が及ぶのかを明確にしておいた方がよいと思う。

事務局：認定を取得した際に、そのサービスで使われているTSA公開鍵証明書に基づいて、認定後に発行されているタイムスタンプが認定の対象になっているという理解である。認定取得後にTSA公開鍵証明書を取り直したり、認定に備えてTSA公開鍵証明書を取得したりすることが考えられるが、認定後に認定を受けたサービスから発行されたタイムスタンプに対して、認定の効果が及ぶものと理解している。認定以前に発行したタイムスタンプまで遡求させるのは少し難しいのではないかと認識している。

伊地知構成員：認定取得後に初めて発行するタイムスタンプに対して、認定の対象とするというようなみなし方をするのが自然ではないか。これについては、EUの場合においても、トラストリストに適格証明書が示されてから、初めて適格タイムスタンプを発行できるという規定になっていたと思う。もう少し深い議論を行う必要があると思うが、現時点ではそのように考えているところである。

西山構成員：サービスの名称について、国の認定を受けた業務のタイムスタンプと、国の認定以前の業務名やサービス名が混同しないような留意が必要ではないかと考えている。

高村参事官：今いただいた論点は、みなし規定を、タイムスタンプの利用を規定する各制度に置くのか、あるいは総務省の認定の告示の方に置くのか、

という制度の立て方に依存する。日本データ通信協会の制度で認定されたタイムスタンプは、いつからいつまでの間、総務省の認定制度に基づき認定されたものとみなすという形で、総務省の告示の方に一括して経過措置としてのみなし規定を置いた場合には、おそらく名称的な差異をつける必要はない。その一方で、電帳法施行規則等の各制度の方で経過措置を置く場合には、いつからいつまでの間はこのように読み替えるという形で、みなし規定を置くことになるので、この場合はおそらく各サービスの方で名称を変えてもらわないとユーザに混乱が生じるのではないかと考えている。いずれにしても、総務省の告示の立て方をどのようにするかということを議論していく中で決まる話になるので、もうしばらく待っていただきたい。

宮崎構成員：資料８－２の11ページについて、今回の制度では、TAA方式とTSAが自ら時刻の信頼性を確保する方式の２つの方式を認定していくことになり、TAA方式は残ることになる。そのときに、TAAの要件として、認定のTAAを利用するということになると考えられるが、TAAは国の認定の対象とならないため、日本データ通信協会は、民間の制度としてTAAの認定制度を今後も継続していくと考えてよいか。

資料８－２の21ページについて、ヨーロッパの場合は、実質的に内部監査を年に１回実施しており、２年間の間にフル監査１回、サーベイランス監査１回、内部監査２回の合計４回の監査が行われているが、日本の場合は、認定のための調査１回、内部監査２回の合計３回の監査・調査が行われるため、ヨーロッパと日本で監査・調査の回数が少し変わってくる。日本における内部監査の内容や報告がこのようになっているので、ヨーロッパの４回の監査に匹敵するようなことができているという説明を用意しておく方がよいと思う。

資料８－２の24ページについて、終了計画は廃止の際に求めるということが記載されているが、資料８－１では、ヨーロッパの場合、認定時に終了計画を確認することになっており、日本でもヨーロッパと同様、認定時に終了計画の中身を確認するというステップを入れた方がよいと考えている。ただし、来年度の制度開始に合わせて、すぐにそれができるかと言うと多分難しい。その前に終了計画とはどのようなもので、このようなことを記載するというガイドライン的なものを整備する必要がある。ただ、将来的には最初の認定の調査時点で終了計画を確認するという方向に持っていけるようにしてほしい。

東條座長：２点目、３点目の指摘は、意見として承った。

伊地知構成員：TAAの認定だけでなく、TSAの認定についても継続される場合が

あるかもしれない。事業者が認定の申請を行っている間については、基本的に制度を続けていく予定である。

高村参事官：終了計画について、しっかりとしたものが必要ではないかという話が先ほどあったが、資料８－１の18ページに、終了計画を適用する際には、５つのステップに則り、対応を行うことが必要となるということが記載されている。実態として、終了計画に記載されていることは廃業するときに利用者に通知する、サービスの引継ぎ先をこのようなプロトコルで探すつもりであるというところまでであり、EUの制度やETSI基準では、終了計画の中でユーザを引き継ぐことが義務化されていない。サービスの引継ぎ先が見つからなければ監督機関が保管義務のあるアーカイブのログ等を保管することで、最終的に担保する形になっている。このような形の終了計画で本当によいのかという部分が一番の考えどころではないかと考えている。以前の検討会で議論したときにも、例えば電気通信事業法の中で、終了計画については事前の届出をさせておらず、実際に廃業するときにどうするのかということを調整しているという話をしたとおり、ユーザのことを考えたときに、ユーザに対しより安全に廃業させることを目指した制度にするのか、あるいは廃業のときのプロセスについて予見性を高めておくことを目指した制度にするのか、どちらがよいのかというバランス論になるのではないかと考えている。

山内構成員：資料８－２の15ページについて、HSMは極めて頑丈なものでなければいけないということが記載されている。また資料８－２の29ページの日本データ通信協会の認定制度と新しい国の認定制度の比較表に、設備面の基準として、FIPS140-2のレベル３認証相当以上に限定せずにコモンクライテリア等の認証制度も活用すると記載されている。他方、電子署名法に基づく特定認証業務の認定の技術基準においては、HSMはFIPS140-1と呼ばれる米国の連邦基準が約20年前に採用されたままで変わっていない。日本データ通信協会の認定制度のような民間の制度でさえもFIPS140-2を使っている中、国の制度である電子署名法に基づく特定認証業務の認定の技術基準がFIPS140-1のままであるのは、整合性の観点で問題があるのではないか。この17年間、指定調査機関として調査を行ってきた実感からすると、現状の電子署名法に基づく特定認証業務の認定の技術基準は陳腐化していると言わざるを得ないと考えている。今回、タイムスタンプで作る制度に併せて、元々の土台となる電子署名法に基づく特定認証業務の認定の技術基準を見直すことが必要ではないか。本件については、先般の「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」においても発言させていただいたが、eシールやリモート署名においても、HSMの技術基

準が非常に重要な問題になってくる。HSMはトラストサービスにおいて極めて重要な技術要素であり、国際相互運用を図る観点でも極めて重要であるので、トラストサービス全体をもう一度眺め直し、国全体としてふさわしい制度設計について考えてほしい。

東條座長：トラストサービス横断的な問題意識として承った。

小松構成員：資料８－２の30ページについて、EUの制度との比較表がまとめられているが、EUで先行している制度とは若干異なるところがある。例えば、自主監査のあり方などはかなり異なる。今、他の会議体でeシールを協議している中で、EUの制度をどのような形で考えていくのかという話が出ている。この比較表はあくまでタイムスタンプを考えた上でのEUの制度との比較であって、現段階でのタイムスタンプのあり方として、このように考えているという形でまとめられていると考えてよいか。eシールの場合、今後、国際的に流通していくということになると、比較的リスクが高い分野になる。タイムスタンプが先行して今回の制度が始まって、そちらの方に引っ張られていくということになると、かなりEUの制度と比べて、監査を含めて制度が物足りないものになるのではないか。

事務局：現段階の国のタイムスタンプ認定制度と、EUの制度との比較であり、参考として記載している。eシールの件とはまた別の話であり、そちらを縛るものではないという認識である。

高村参事官：ヨーロッパとの制度整合性、お互いで作ったものがお互いの国で流通するようにするためには、どうすればよいかということについて考えていると理解した。日本政府全体の立場としては、先ずは日本国としてどのような制度を作るかを考えたい。それを運用しつつ、その中でEUと相互にお互いのものを流通させてもよいかというところについて合意に達するという形が基本的には正しい姿であると考えている。現在、EUがeIDAS規則に基づく制度という形で作っているものに比べて、今回の日本の新しい国の認定制度という形で比較表に記載しているものは、一部緩いところがあるという指摘はごもっともであり、それをEUが許してくれるかどうかもよく分からない。いずれにせよGDPRのときにお互いの個人情報保護法が若干制度のずれがあるという状況の中で、十分性認定という形での合意に達したのと同じように、なるべく今作ろうとしている国の認定制度を変えない形でEUと合意することができればよいのではないかと考えている。先ほどeシールの話が出たが、eシールとタイムスタンプの中で決定的な違いがあるとすると、既にEUに制度があるというよりは、EU側が既にある国際標準を無視して新しい国際標準を作っているところにあると考えている。今、日本国内で流通しているタイムスタンプは、RFC3161という形で国際

標準化されたものを使っているが、EUはわざわざ自分たちのeIDAS規則のために別の国際標準を作っており、技術的な整合性は取れていない。技術的整合性が取れていないことを前提として、お互いに相互認証をどのようにしていくかという議論になり、その部分が決定的に違うのではないかと考えている。同じように、例えば、PDFに関する電子署名についても、日本や米国ではISO 32000-1に従ったものが使われているが、EUでは勝手にその基準をいじって、コンパチビリティをなくしたうえでETSIの基準を作っている。今、EUのために、ISO 32000-2を作るかどうかをISOで議論しているような状況である。EU側がわざと国際標準に合致しない制度を作ってきたという実態があるので、その部分を含めて、国際相互認証としてはどうあるべきかという議論を行っていく必要があるのではないかと考えている。

伊地知構成員：資料８－２の27ページについて、法令・ガイドライン等における認定タイムスタンプの位置づけが記載されているが、この中のガイドライン等については、日本データ通信協会の認定するタイムスタンプ等、同協会の名前が入った形でガイドライン等が示されていると思う。この部分については、国の認定制度ということが早いタイミングで明確に書かれる必要があると考えている。検討会の構成員の中には、いろいろなガイドライン等に深く関わっている方々が多数いらっしゃるように思う。ぜひ、そのような対応を促進するような動きをしてもらいたい。

岩間構成員：調査と監査という言い方に違和感がある。申請してもらったものに対して審査して認定を付与する、あるいは認証するという形が一般的であると考えられるが、これは審査ではなく、調査という言葉を使っているのには、何か理由があるか。

高村参事官：法律上、調査の結果等何らか出てきたもので判断するという場合には審査に該当する。それに対して、今回の認定制度の場合は、ファシリティ面等については実際に現地に出向いたりするという追加の部分が入ってくるので、調査という書き方をしている。皆様が思われているいわゆる審査というものが、法律上は調査という表現になると理解してもらいたい。なお、この書きぶりは電子署名法と同じ書き方であると理解してもらいたい。

東條座長：法律上の話であればやむを得ない。検討会取りまとめ骨子（案）については、概ねこれまでに検討いただいたことをまとめたという内容になっているので、皆様に賛同いただいたということで、次回は、今回いただいた意見と合意いただいた内容を踏まえ、事務局にて整理のうえ取りまとめ案を提示いただく予定である。

⑤その他

事務局から、次回の日程について別途メールで案内する旨の説明があった。

（３）閉会

以上