参考資料７－５

タイムスタンプ認定制度に関する検討会（第６回）

１　日　時

令和２年９月 23 日（水）16:00～17:35

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、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、若目田構成員

（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、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）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６－１　タイムスタンプ認定制度に関する検討会（第６回）事務局資料
資料６－２　日本データ通信協会提出資料
参考資料６－１　タイムスタンプ認定制度に関する検討会（第５回）議事要旨

５　議事要旨

（１）開　会

（２）議　題

①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６－１について事務局から、資料６－２について伊地知構成員から説明があった。

②意見交換

主な意見等は次のとおり。

東條座長：まず１点目だが、「TSAが自ら時刻の信頼性を確保する方式」について意見交換をお願いする。

宮崎構成員：資料６－２の２ページ目、５ページ目、６ページ目にあるタイムスタンプ発行前の時刻精度の確認について、これは現行の日本の制度では、タイムスタンプトークンを発行する前にスタンプの中に記載された時刻をチェックするという手順を取っているが、このことを指しているのか

伊地知構成員：日本データ通信協会の認定制度の中でも、タイムスタンプ発行前の時刻精度の確認については、具体的な方法を特定しているものではない。タイムスタンプトークンを生成した後に時刻をチェックするという方式もあれば、別の方法でタイムスタンプサーバーの時刻を定期的にチェックするという方式もある。

宮崎構成員：タイムスタンプユニットの時刻を定期的にチェックするということでもよいとなるとかなり幅広く方式を認めるということになる。

東條座長：このような方式がよいという提案はあるか。

宮崎構成員：幅広く方式を認めるという方向でよいと考えている。資料の文面だけ読むとそのような方向であるかが曖昧であったため、質問させていただいた。資料の文面は修正した方がよい。

東條座長：報告書を作成する際には、工夫させていただきたいと思う。

宮崎構成員：資料６－２の６ページに、具体的な審査基準検討の場と記載されているが、想定されているものはあるか。

伊地知構成員：総務省の委託事業を、野村総合研究所が担当していて、この委託事業の中に、審査基準の案の作成という項目が含まれている。委託事業の中で、具体的な審査基準の検討を始めるという計画があることを承知している。

事務局：総務省の委託事業を野村総合研究所に担当してもらっている。国としての認定制度はこの検討会で議論することになっているが、細かい審査基準等については、委託事業も活用しながら、日本データ通信協会の専門家の皆様にも参加していただいて議論していくという認識である。

小田嶋構成員：資料６－２の６ページのログ等の保管について、おそらくログだけではなく、証票類も含めることになると考えているが、こちらは電子署名法施行規則の第１２条第１項第４号あたりが参考になると考えている。

東條座長：続いて、「認定の有効期間」について意見交換をお願いする。

宮崎構成員：鍵更新が監査や審査と連動していないことは、欧州の状況を教えてもらって、よく分かった。その際、欧州では、鍵更新を行ったことをトラストリストの責任組織に対して自己申告するということを伺った。加えて、監査や審査の際に、鍵が更新されたということについてエビデンスを残しておいてチェックする。エビデンスを残す元となる鍵更新自体をデュ

アルコントロールのような形で二重チェックする。このような運用を現実的に行っていることが分かったので、そのような方向でよいと考えている。ただそれで安全であるかというと、不安があるため、タイムスタンプトークンのサンプリングチェックを検討した方がよいのではないか。

伊地知構成員：サンプリングチェックについては、TUVITへのヒアリングの中で実施していることが分かった。またそれ以前に日本の中で検討する際にも、いろいろな方々がアイデアとして提示していたので、前向きに検討してもよいのではないかと考えている。適切な方法だと考えている。

東條座長：サンプリングチェックについて検討に加えることとする。

西山構成員：資料６－２の７ページに関わるが、鍵更新の際に、デュアルコントロールでチェックを行うということであるが、鍵の廃棄については、どのような形で確認して記録を残しているかが気になったので、教えてほしい。

伊地知構成員：鍵の廃棄についても、HSMの操作のキャプチャー画面などを確認し、それがエビデンスとしても残されているので、報告書や作業記録を現地で確認している。

西山構成員：おそらく現行の方法で問題はないと思われるが、実際にルールを作る際には、鍵の廃棄も重要なファクターになるので、報告書に鍵の廃棄についても言及しておいた方がよい。

東條座長：第３の論点である「監査の在り方」について意見交換をお願いする。

宮崎構成員：内部監査レポートのようなものの提出を義務付けるという方向になるか。また、内部監査レポートの内容についても予め規定しておくという方向になるか。

伊地知構成員：監査の報告に関する具体的な提出物などについては、具体的な審査基準検討の場で議論することになるテーマであると考えている。日本データ通信協会の認定制度の中では、審査基準の横に記述ができるようになっている別紙のようなものがある。審査基準の全項目に対して、監査人がチェックを行った内容やその評価を記載してもらったものとそのサマリーレポートを併せてエビデンスとして提示してもらっている。

上原構成員：内部監査の客観性が気になっている。現行の制度では内部監査は問題ないかもしれないが、今後広く事業者に参入してもらうことを想定しなければいけない。現行の限られた事業者の活動については信用できるかもしれないが、それ以外の事業者については、限られた事業者と同じような目線で信用して動くとは思えないので、疑問に感じる。

東條座長：プレイヤーが増えてきたときに、信頼性を確保できるかどうかという質問であると受け取った。

伊地知構成員：若干信頼性に疑問が残るという部分については、ご指摘のとおりであると考えている。今の状況で考えて、制度をどのように設計するかということや、将来にわたってこの制度のままでよいのかということなど、いろいろな観点で議論することが必要であると考えている。

東條座長：将来的な課題として位置付ける。

小松構成員：内部監査については何らかの監査の基準があり、その中には、独立性の確保のため、どのような人が監査を行うかなどが規定され、評価基準や監査の手順・手続きについても、設定されるということでよいか。

伊地知構成員：現行の制度においては、独立性の確保などを審査基準の中で明確に規定している。評価基準についても、審査基準を用いた監査を行うということを規定している。一方で、監査の手順・手続きについては、言及がない。審査基準検討の場では、ご指摘を踏まえて、もう少し詳細化する必要がある部分も出てくると思う。

岩間構成員：ISO/IEC 17025では、内部監査において、どのような項目を報告する必要があるかといった部分を規定している。そのあたりを参考にして、内部監査において、どのような内容の報告を求めるか、どのようなエビデンスの提示を求めるかといった部分を規定した方がよい。

伊地知構成員：日本データ通信協会の審査基準の中では、ISO/IEC 17025を参照する形にはなっていない。今後の制度化にあたっては、そのような国際規格があれば活用すべきであると認識。

山内構成員：今回議論しているものは組織の認定ではなく、サービスの認定であると理解している。TSAが行う時刻認証業務、サービスを審査して評価して認定することになる。ただ、組織としてのTSAがしっかりとマネジメントシステムを回していることが大事である。そのときに、基本的なマネジメントシステムを回すという部分を、内部監査で実施してもらうということも１つのアイデアではないか。マネジメントシステムの内部監査は、ISO/IEC 19011という国際規格に規定されている。ISOのマネジメントシステムの認証を受ける組織は、認証機関の認証審査を受ける前に、定期的に内部監査を実施している。そのときにISO/IEC 19011を使っていることが多いので、内部監査に関する基準を日本データ通信協会の有識者メンバーで検討する際には、それを参考にしてはどうか。

東條座長：今の意見は、TSAの組織のマネジメントやガバナンスに関する監査の話になるか。

山内構成員：そのような認識である。内部監査は、TSA自身が内部監査を行って、認定する際に、審査機関がその内部監査の結果をチェックするという話であると理解した。その内部監査の方法については、ISO/IECの世界で

は、ISO/IEC 19011という方法がある。

伊地知構成員：先ほどISO/IEC 17025という話もあったので、頂いた情報について、内容を確認して参考にすべきであると考えている。

山内構成員：ISO/IEC 17025は、参考にするべきところはあると思うが、試験所認定の国際規格である。

伊地知構成員：審査基準検討の場は、日本データ通信協会が設けるものではなく、総務省の委託事業の中で実施されるものであることを改めて補足。

上原構成員：審査の際に内部監査の結果をもちろん見ることになるが、先ほどの話では、別紙のチェックリストのようなものに監査人がチェックを行った内容やその評価を記載し、それを提出してもらって確認しているという話であった。その部分に対しては、実質上、証拠類を保管させたり、必要になればそれを出して見ることができたり、更に気になるところがあれば、外部監査を入れてチェックするという仕組みがあった方がよいのではないか。

伊地知構成員：現行の制度では、チェックリストのようなものを提出してもらっていると説明したが、実際には、監査人が背後の証拠類についてもチェックを行い、内部監査を行っているという状況である。気になるところがあれば、外部監査を入れるという部分については、現行の制度では、内部監査の結果の報告を受けたときに、大きな問題があるという認識をすれば、調査を行うという仕組みになっている。今後の国の制度の中では、外部監査を入れるという可能性についても検討してもよいのではないかと考えている。

東條座長：それでは、最後に「廃止の場合の取扱い」について意見交換をお願いする。

吉田構成員：資料６－２の11ページに、現時点では業務廃止時及び廃止後に問題は発生していないと記載されているが、どのようなケースにおいて問題がないと言っているのか確認したい。

伊地知構成員：現行の制度の中では、タイムスタンプトークンを検証する上で問題がないという意味合いで記載している。

吉田構成員：タイムスタンプはこれからのデジタル社会における重要なトラストアンカーであり、今後、タイムスタンプを押す件数も増えてくると想定される。今後を見据え、どのような問題があるかを踏まえ、制度設計を行ってほしい。

EUの終了計画の話は非常に良い話であると考えている。利用者の観点から、事前に廃止を申告しなければならないという制度になればよい。実際に使っていたユーザはどうするのかという部分は終了計画に盛り込んだ

方がよい。事業認定を行う際に、終了計画も併せて認定するような仕組みも検討してほしい。

伊地知構成員：EUの終了計画については、タイムスタンプの関係者の中でも非常に有用であるという認識を持っている。終了計画を審査基準に定めることについて検討すべきである。一方で、終了計画を設けることのみを審査基準にしても、実態として適切な終了計画が策定されるかどうかが分からないので、ENISAが公表している終了計画のガイドラインのようなものを業界団体と早急に検討することも非常に重要であると認識している。

宮崎構成員：廃業の届出について、事後では不適ではないか。トラストリストを検証時のトラストアンカーとして使うことを見据えると、廃止のステータスを速やかに反映しておかないといけない。そうでないと、検証システムが間違った検証結果を示してしまう可能性がある。今回の検討にあたってはトラストリストへの反映を予め勘案したような運用の仕組みや審査基準が必要になると考えているため、事後で問題がなかったという話ではなく、事前に届出を行うことを義務付けるべき。どれぐらい前に届出を行うかということについては、トラストリストの運用や更新するタイミングとの兼ね合いで判断する必要がある。

　終了計画については、エンドユーザを保護する意味で、まず有用である。また、ベンダー自身も、終了にあたって実施すべき事項や工数を把握することで計画を立てやすくなるのではないか。ENISAのガイドラインのようなものを日本でも用意して、それに基づいて審査のときに提出してもらうことを検討すべき。

伊地知構成員：トラストリストの運用の観点で事後の届出では不適である点については、同意する。一方でトラストリストの運用については、具体的な規定をどこかで別途定める必要があると考えているので、事前の届出をこの業務の廃止に関する規定の中だけで謳うということではなく、別に定め得る場所があるのではないかと考えている。そのようなことを踏まえると、事後ということにこだわっている訳ではない。ただ、日本データ通信協会の制度が、なぜ事後になっているかという点については、聞く話によると、事業者の方の不都合、具体的には事前に申請を出し了承されてからでないと廃止できないという部分については手続き上、さまざまな負担があるのではないかという声があったことは補足しておきたい。

東條座長：事前、事後のどちらもあり得るということか。それとも今の意見を踏まえて、事前の方が適切であるということか。もう少し明確にしてほしい。

伊地知構成員：他に不都合がなければ、事前について否定するものではない。

東條座長：それを踏まえて、引き続き検討することとする。先ほど意見が出ていたこの検討会の場で審査基準そのものを検討するのかという点について、今後のスケジュールの話もあるので、事務局に感触を伺いたい。

事務局：どこまで細かく議論するのかという話がある。日本データ通信協会の有識者を含めた具体的な審査基準検討の場で細かい基準について議論することが適切であると考えている。

西山構成員：廃止の届出については、事前の通知が必要であると考えている。トラストリストの記載という話もあるが、トラストリストがなくても、認定認証業務では、認定認証事業者を主務３省のホームページで公開している。突然廃業して事後に通知されると、認定認証業務として公開されているにもかかわらず、実際には廃業していたということになるので、そういうことがないように事前の届出が制度として規定されている。従ってトラストリストができれば尚更よいが、現行の制度の中でも事前の届出がふさわしいのではないか。

　認証局がタイムスタンプ局用の証明書を発行しているが、EUで運用されているルールを適用すると、廃業したタイムスタンプ局用の証明書は失効処理を行うことになる。失効処理を行うとタイムスタンプの検証ができなくなるので、失効処理を行わなくてもよい理由付けが必要になる。そうすると、このような理由で廃業するが、事前に秘密鍵は廃棄しているから、失効の必要はないという話を事前にもらう必要がある。現行の日本データ通信協会の認定制度の中でも、そういうことであるということで運用されているが、国の認定制度になれば、このあたりを少し明文化してルール化した方がよいと考えているため、事前の届出は必要になると考えている。それと同じく、終了計画も重要な要素になる。

伊地知構成員：廃止の際に鍵の廃棄が重要であることはご指摘のとおり。一方で実際に失効させるか否かについては、検証のプロセスがどのように作られて、それがどう普及しているのかという状況との兼ね合いがある話になる。単に基準として方向を決めるだけでは、なかなか実態として上手くいかないという点もあるのではないかということを危惧している。基準についても真剣な議論が必要であるが、それと併せて検証のプロセスをどのような形で作るべきであるのかということも、具体的な案を示す必要があるのではないかと考えている。

東條座長：国の制度を作る際には、このあたりについて丁寧に検討した方がよい。

高村参事官：いわゆる退出規制を考える際に、利用者からみて予見性が高い方がよいという話はそのとおりである。その一方で、退出したいと考えてい

る事業者が、終了計画を遂行できるだけの体力が残っているかどうかといった問題も併せて考えなくてはならないと考えている。非常に手厚い終了計画を作っていて、認定の段階ではそれをやり遂げる体力を備えていたが、認定期間の間に経営状況が極めて急速に悪化した場合に、安全に事業を廃止させなければならない可能性もある。そのときに事前に作った手厚い終了計画を信じて契約していた契約者からみると、終了計画が手厚いがゆえに、別のサービスにスイッチする準備が出来ていないケースが想定されるので、退出規制の部分を緩くするのか、厳しくするのかはかなりデリケートな話になる。今まで総務省が取り組んできた業務についてみると、例えば、ポケットベルを終了させるために、何十年も要した。ニーズは少ないが、利用者が存在する中で、すべてのサービスを終了させるには、少しずつ別の事業者に移行をかけながらやめていくという形を採っている。事前に終了計画をオープンにしているだけで利用者にとって安全なサービスとなるのか、それとも終了計画自体については、認定の段階で定めている訳ではないが、資料６－２の13ページ目の電気通信事業法に記載しているとおり利用者の利益を保護するための必要な事項の周知として、その周知期間について事業者と国が相談しながら適正な期間を定めたうえでソフトランディングを図っていくのか、どちらがよいのかを考える必要がある。終了計画を作ることは予見性を高めるうえではよいことであるが、終了計画を利用者が信じている中で終了計画を遂行できないときにどうなるのかというリスクを含めて、どうあるべきかを検討してほしい。なお、日本データ通信協会の制度で退出規制の記述が緩くなっているのは、日本データ通信協会の場合には認定は行っているが、退出することを宣言されてしまったときに、対抗手段がないからである。そういうことを踏まえて、厳しい基準がかかっていないことを理解してほしい。

東條座長：退出規制の問題は扱いが大変デリケートであると認識。

山内構成員：資料６－２の15ページについて、言葉遣いが不明確。論点のところに、TSAの業務廃止の際の届出については、事前とすることが適切かという記載があるが、誰に対して届出を行うのかといった記載がされていない。方向性に関する見解のところにも、廃止後に遅滞なく届出を求めることで十分ではないかという記載があるが、誰に対しての届出を求めるのかが記載されていないので、混乱しているような気がする。もし、国の制度になるのであれば、主務省に対して、廃止後に終了したことを伝えられても遅いので、ガイドラインなどの何らかの仕組みを検討する必要があるのではないか。事業として継続できそうにないということを、TSAが総務省や日本データ通信協会と事前に相談して、問題がないようにするべきであ

る。あくまでこの制度は、TSAのためにある訳ではなく、TSAのタイムスタンプを利用するユーザ企業や第三者であるリライングパーティがタイムスタンプを検証することによって、安全に電子文書を使っていくという社会全般のためにあるものである。

上原構成員：廃業後タイムスタンプは検証できない、となると証拠性もないものになってしまうため、非常につらい。何らかの形できちんと引き継ぐなり、何かすることが必要である。手厚い終了計画といっても、継続性について、このように考えているというレベルでもよいので、終了計画は必要ではないかと考えている。

高村参事官：誰に引き継ぐという話が必要ではないかという話が出たが、その部分を必須化してしまうと、業界最安値でサービスを実施している事業者においては、同じ条件で契約を引き継げないという問題も出てくるので、終了計画はなかなかデリケートなものである。いずれにせよ必要であればそれを求めなければならない。認定の基準を厳しくすることが必要になるかもしれない。何が必要であるかは構成員の皆様に議論を賜りたい。退出規制については、こうあるべきという理想論と、事業者が廃止をしたいと思っているときの動機のバランスを考えると難しいところがある。そのデリケートな部分のバランスを取る必要があることを念頭に置いて、議論を賜りたい。廃業によって、有効期限内のタイムスタンプを検証できなくなってしまうという事態は避けなければならないという指摘はそのとおり。そういった部分をどのように担保するかは、構成員の皆様にお知恵を拝借したい。

柿崎構成員：廃止後に遅滞なく届出を求めるということについては、トラストリストに掲載することが間に合わないという問題があるので、事前の通知が必要であると考えている。トラストリストに掲載されている情報でタイムスタンプが有効であるのか、認定を受けた適切なタイムスタンプであるのかを検証できることが重要であるので、予めトラストリストの方にこれ以降は業務廃止になるということがきちんと記載されることが重要であると考えている。

　終了計画については、資料６－２の14ページに記載されているEUの要件でほぼ十分ではないかと考えている。例えば、サービス廃止の３か月前までに監督機関に報告と記載されており、期間については議論があるが、適当な期間までに事前に報告しなければならない。利用者に対して、サービス廃止の旨を通知しなければならない。タイムスタンプを事後において検証できるように、TSA公開鍵証明書等の必要な情報について適切に保管して、他の事業者に移行したり、トラストリストに掲載したりすることをし

なければならない。この程度の終了計画については、きちんと規定した方がよいと考えている。

小田嶋構成員：廃止の場合の取扱いについては、トラストリストへの速やかな掲載が必要であると考えている。これは署名検証者への告知を含めて考えると、国への届出になると考えているが、併せて利用者や署名検証者への告知は同時でもよいと考えている。電子署名法の場合は、60日前までに利用者へ通知することを運用規程に記載することになっている（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に係る指針第１２条第２項）。

梅本構成員：利用者の便宜のためには、利用者に対して、何らか十分な情報を提供する必要があると考えている。かっちりした終了計画は難しいとしても、少なくともサービス廃止の通知のときに、自分が受け取っている既発行のタイムスタンプがどうなるのかという説明を伝えるように努めるという努力義務の規定を入れてもよいのではないかと考えている。また廃止の際に引き継ぎが起こるケースや、廃止しなくても、合併により、サービスの統合が起こるケースも出てくるので、そのような場合のプロセスを何らか定めておいた方がよいのではないかと考えている。

吉田構成員：現在、日本ではWi-Fiの料金設定で揉めているといった状況もあるので、センシティブな問題である。審査基準について、この検討会で議論した方がよいと考えている理由の一つは、例えば、欧州の場合、TSPのバックアップを国が担っているところもあり、今回の制度では国がバックアップするかというとそうではないと考えているが、継続性を保証するうえで保険の活用を基準として規定するという方法もあるという意図によるものである。

伊地知構成員：保険の活用もぜひできるようになるとよいと考えている。経験談としては、タイムスタンプの認定制度が出来る頃の十四、五年前の話になるが、日本の損害保険会社がこのような保険を作ることに対し、取り組みにくい環境がまだあった。これからはタイムスタンプも普及していくという状況になっているので、このような保険ができることを期待したい。

小田嶋構成員：事業体として求められる要件に関連するが、財務状況の報告の頻度を、例えば１年に１回としたり、半年に１回としたりすることで、少なくとも想定外の廃止に至ることがないようにすることができればよいと考えている。また保険の活用に関して、現在、サイバーセキュリティ保険が提供されており、電子認証局会議において、電子署名法に基づく特定認証業務の相当数が、そのような保険に加入しているということを把握しているので、お伝えしたい。

東條座長：TSAが自ら時刻の信頼性を確保する方式については、資料６－２の６ページに記載されているとおり、「NICT」のUTC（NICT）に対してトレーサブルであることを求める、かつトレーサビリティの起点となる時刻源±１秒以内とする、タイムスタンプ発行前に時刻精度の確認を行う、適切な機器における適切なログの保管を規定することが望ましい、ということについて取りまとめを行うこととする。

認定の有効期間については、資料６－２の８ページに記載されているとおり、認定の有効期間は２年でよいということについて取りまとめを行うこととする。

監査の在り方については、いろいろな意見が出たが、方向性としては資料６－２の10ページに記載されているとおり、内部監査も認めるということについて、取りまとめを行うことでよいと思う。なお、必要に応じて外部監査も入れるということ。また、監査の頻度についても年に１回と規定することについて、取りまとめを行うことでよい。特に御異論がなかったと承知している。

廃止の場合の取扱いについては、資料６－２の15ページに廃止後に遅滞なく届出を求めると記載されていたが、その方向性とは異なり、構成員の皆様の意見を踏まえて、事前の届出を求める、終了計画の提出も求め、事前に審査することが重要である。一方で、退出規制については、なかなかデリケートな問題もあり、規制サイドが想定したような制度設計が必ずしも実態として利用者の保護に繋がるとは限らないという悩ましい問題もあることが確認された。今後も引き続き、最も望ましい利用者視点の制度設計について検討していきたいと考えている。以上について取りまとめをさせていただく。

③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