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）

１　日　時

令和２年８月７日（金）16:00～17:10

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５－１　タイムスタンプ認定制度に関する検討会（第５回）事務局資料
資料５－２　日本データ通信協会提出資料
参考資料５－１　タイムスタンプ認定制度に関する検討会（第４回）議事要旨

５　議事要旨

（１）開　会

田原サイバーセキュリティ統括官から挨拶。
藤野サイバーセキュリティ統括官室審議官から挨拶。
中溝サイバーセキュリティ統括官室参事官（総括担当）から挨拶。
高村サイバーセキュリティ統括官室参事官（政策担当）から挨拶。
海野サイバーセキュリティ統括官室参事官（国際担当）から挨拶。

（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５－１について事務局から、資料５－２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：認定業務の公表内容及び公表方法について、構成員の皆様の御意見を頂戴したい。

宮崎構成員：資料５－２の１ページ目の課題について、１つのTSAが認定のタイムスタンプと非認定のタイムスタンプを発行している場合があり、それらを区別するのが困難であるとの説明があった。もちろんそれも困難であるが、当該TSAが発行したかどうかをエンドユーザが認識することも困難である。タイムスタンプトークンに入っている発行者の公開鍵証明書やタイムスタンプを発行するにあたってのポリシーのIDは全く同じものを容易に偽造することができてしまう。唯一偽造できないのは鍵ペアである。機械処理が困難であること以外にも、そのような問題がある。

資料５－２の３ページ目の公表している項目について、履歴情報が重要な項目として抜けている。この業務はいつまで認定を受けていたが、それ以降は認定を受けていないという履歴情報も重要。

伊地知構成員：タイムスタンプトークンに施されているデジタル署名を検証することによって、タイムスタンプを発行した事業者を特定することができる。実際にそのタイムスタンプトークンが認定の業務に係るものであるかどうかについては、今のところ、日本データ通信協会の方ではその情報を公開していないため、その部分の確認はできない。

宮崎構成員：TSA公開鍵証明書を見れば、どのCAが証明書を発行して、どのTSAが発行を受けたのかが分かるが、全く同じものを簡単に偽造することができてしまう。確かな認証局のルート証明書、これがトラストアンカーであるが、そのルート証明書が正しいということが何らかの手段で確認できる状況であれば、そのルート証明書から辿って、下位の証明書を検証することで、この証明書が正しいということが分かる。そのときに、どのルートを辿って、そのルート証明書が正しいということをエンドユーザが認識できるかという部分が非常に重要になる。

東條座長：本日の検討対象との関係でみると、どのような議論に繋がることになるか。

宮崎構成員：トラストリストに何を含めるかという議論に繋がる。EUのトラストリストのようにデジタルIDである公開鍵証明書そのものを偽造できない形で公表し、誰でもアクセスできるようにすることができれば、懸念は生じない。

小田嶋構成員：資料５－２の８ページの公表内容及び公表方法について、法人

番号を公表内容に含めるべきであると考えている。平成27年の各府省の情報化統括責任者連絡会議で、公開情報への法人番号の併記を求められるようになっている。公表内容を公開情報として考えると、法人番号を含める形で併記が必要になる。タイムスタンプ業務の名称と業務を行う者の名称の２つはセットになると考えている。今後、海外との連携を想定すると、英文の情報も想定すべきである。

宮崎構成員：資料５－２の８ページの公表内容及び公表方法について、何のための公表であるかという部分については、人間が読むためのもの、機械が読むためのものの２つがある。人間が読む場合はどの事業者が認定を受けているかということが分かるが、それ以上のことは分からない。機械が読む場合、タイムスタンプトークンが認定を受けているものかどうかを区別できなければならない。

タイムスタンプは電子署名と組み合わせて、長期署名として使われることが一般的であることを踏まえると、電子署名そのものの信頼性も同時に示された方がよい。トラストリストに掲載し、タイムスタンプに加え電子署名についても１つのデータとして参照されるようになっていると、長期署名の検証の際に、タイムスタンプと電子署名について別々にトラストアンカーの情報を取ってくる必要はなくなる。同じ枠組みの中で、信頼できるものとして双方を公開することが望まれる。

資料５－２の３ページの公表している項目において、履歴情報が重要であるという話をしたが、長期署名を検証する場合、その長期署名というデータの中には、検証のためのデータが詰まっているため、過去の情報も含めて検証できるようになっている。唯一できないのは、過去のトラストアンカーとされていたものが、過去の時点で本当に正しかったのかを確認することである。それが弱点であったため、エンドユーザが独自の形で、過去のトラストアンカーというものを管理しておかなければならなかった。トラストリストの中で、過去の履歴も含めて蓄積できるような形でリスト化していけば、長期署名の検証にも資する。トラストリストはEUでは標準化され、Adobeのリーダーでも読むことができる。日本でトラストリストを考える場合においても、EUと同じ形式を採用すれば、様々なところで利用しやすくなる。今年度から、WIPOが知財保護に有益であるということでTSA業務を始めたように、世界的に知財保護の領域でタイムスタンプが使われるようになってくると海外との相互運用や相互承認がますます重要になるのではないか。

東條座長：資料５－２の８ページの公表内容及び公表方法の参考のところだがマシンリーダブルか、ヒューマンリーダブルかという話で、EUは法令でマ

シンリーダブルな形式が必須であるということを義務付けているが今後、丁寧な検討が必要であるという説明があった。この点について、御意見を頂戴したい。

伊地知構成員：現状としては、電子帳簿保存法等において日本データ通信協会が認定するタイムスタンプと記載されているので、どの事業者が認定を受けているのか確認する意味合いで人間が読むことを想定している。一方でタイムスタンプトークン個々をどのように識別するかという部分は、TSA公開鍵証明書で確認する必要がある。

長期署名の中では、タイムスタンプも電子署名も両方使われるので、トラストリストに電子署名も含めるべきであるという点については、トラストサービス横断的なトラストリストということで、丁寧な設計を行うことが必要であると認識している。

東條座長：マシンリーダブルでないと、現実的に照合ができないのではないかという御意見を頂戴していたと思うが、その部分についてどうか。

宮崎構成員：例えば、このタイムスタンプトークンが認定を受けたものであるかという確認を行う手掛かりとして、電子署名法では、ルート証明書のハッシュ値を官報に掲載している。手元にある公開鍵証明書のハッシュ値と官報に掲載された文字の並びを比べると照合できる。もっとも、実際にはそのようなことを行う人はほとんどいない。機械たる検証ソフトが、トラストアンカーとして、トラストリストのような検証に必要なデータを持っていれば、その検証ソフトがユーザーからの求めに応じて、認定を受けたタイムスタンプであるかどうかを示す。そのような使われ方が一般的になるのではないかと考えている。マシンリーダブルであるということは、結果的にヒューマンリーダブルでの表示もできる。EUがマシンリーダブルを必須にして、ヒューマンリーダブルをオプションにしているのは、そういう背景がある。

上原構成員：電子署名とタイムスタンプの両方のサービスを使う場合、それぞれの監督省庁の別のページを見ないといけないとなるとユーザーには面倒である。EUのトラストリストのように１箇所で共通で見ることができるようになっているのが理想。

事務局：電子署名については、総務省、法務省及び経済産業省のそれぞれが、タイムスタンプについては、総務省がホームページにおいて情報を提供している。

今後、更にタイムスタンプの公開鍵証明書の情報を掲載するとなると、そのような情報も含めて１箇所で共通で見ることができるようにすることが重要と認識。

西山構成員：資料５－２の８ページの公表内容及び公表方法について、TSAの公開鍵証明書等の一意にタイムスタンプサービスを特定可能な情報等の公表と、当該TSAの公開鍵証明書を特定できる認証局の証明書の公開の話が記載されているが、どちらも必要であると考えている。但し一長一短あるのではないか。例えば、タイムスタンプ局のある一つの公開鍵証明書と鍵ペアにスコープを当て、ある特定の認証局から発行された鍵ペアに基づいて発行しているタイムスタンプがあるとすると、その認証局が廃業した場合に、タイムスタンプが検証できなくなる可能性がある。タイムスタンプを検証するときに、認証局の失効情報を参照するが、その認証局が廃業した場合には失効情報を見ることができなくなるため、タイムスタンプが検証できなくなる。

TSAによっては数十種類のタイムスタンプ局用証明書を毎年更新している。タイムスタンプの有効期間は10年であるから、10～20年の運用でみると数百種類のタイムスタンプ局用の証明書が存在する。そのうちの一部のタイムスタンプ局用の証明書については、有効性が確認できない場合が想定される。従ってそのような履歴を追うことができる形で公開を行うということが適切になってくる。そういうことを踏まえて、どういう内容のものを公開していくか考える必要がある。

一方で、認証局の証明書を公開する場合にはその認証局が閉局となったときにそれを外せばよいので、それだけで済む。そういった特色がある。

柿崎構成員：トラストリストに記載されている情報、タイムスタンプトークン、文書、それら３点セットを使って、機械やコンピュータ、ソフトウェアがそのタイムスタンプが本当に認定されたものであるか、またそれが有効であるのかを検証できる情報が公表されていることが一番重要。公開鍵証明書のハッシュ値だけだと、公開鍵証明書を特定するという段階から検証しなくてはならないため、公開鍵証明書全体を公開するのが望ましい。

梅本構成員：マシンリーダブルとヒューマンリーダブルは活用の場面が異なるため、いずれも重要なのではないか。マシンリーダブルは既に発行されているタイムスタンプの自動的な検証のために必要である。これに対し、ヒューマンリーダブルは、これからタイムスタンプを導入しようとしている会社がサービス選択を行うときの一つの手掛かりとなる情報として使うことになるのでは。そのような観点からみると、法人情報は事業者をユニークに特定するための情報として必要である。利用者からみると、認定を受けてからどれぐらい時間が経過しているのかといった情報が必要であり、適切な実績がある企業であるのかを判断するために、最初の認定日も掲載されている方がよい。他方で、日本データ通信協会の現在の公表情報

に入っている代表者名はユーザーにとってそれほど重要な情報ではないので掲載する必要はないのではないか。

吉田構成員：事業者名の開示について、漢字表記で出す訳にはいかない。法人番号と関連するが、アルファベットの商号表記でもって、事業者名を公表してほしい。法人番号については、データ流通をさせるときにこれをどう使うかを真面目に検討しなければいけない。産業界毎に考えると、資料５－２の８ページの公表内容の一つとして、例えば、金融分野等で使われているLEI（取引主体識別子）のような番号をオプションとして必要ではないかと考えている。併せて検討してほしい。

岩間構成員：履歴という話が出たが、例えば、TSAが廃業した場合でもトラストリストにその情報を残しておくのか。長期署名の検証のためには、そのような情報を当然残しておいた方がよいが、いつまで残しておいた方がよいのか。そのような部分はトラストリストの作り方にもいろいろと影響があるので検討が必要であると考えている。

上原構成員：製薬業界では特許の有効期間中プラスアルファという非常に長い期間、データを管理しておく必要がある。20年前の会社がずっと存続していればよいが、存続していなかったとしても、その会社が提供してきたデータにタイムスタンプが付いていて、その会社のタイムスタンプについて後になって万が一裁判になったときでも大丈夫であると言うために確認できるような状態にしてもらいたい。

伊地知構成員：適切な検証ができる情報があればよいという話が出たが、非常に分かりやすい整理であると思う。公開鍵証明書のハッシュ値だけでなく、公開鍵証明書もあった方がよいという話が出たが、この部分も当然そういうことであると思う。マシンリーダブルは、既に発行されているタイムスタンプの自動的な検証に使われるが、ヒューマンリーダブルはこれからタイムスタンプを導入しようとするときのサービスの選択に使われる。特に電子帳簿保存法や、INPITのタイムスタンプ保管サービスなどは日本データ通信協会が認定するタイムスタンプという条件が付いている。そういったことを目的に利用するユーザーが間違いなく選択できるという意味では、どの事業者のどのサービスが認定を受けているのかという情報がしっかりと掲載される必要がある。

トラストリストでもって、履歴情報を用いて長期にわたって検証できるような環境を提供することが、非常に要望の強い部分であるということを認識している。

タイムスタンプの業界では、タイムスタンプ局自体の廃業、それに引き続いて認証局自体の廃業という事例もあり、対応についてどうするべきか

という検討を業界挙げて行った経緯もある。その際の反省点や検討した内容なども踏まえて、今後、トラストリストの丁寧な設計が必要であるという部分に役立てていくのがよいのではないかと考えている。事業者名の英文表記についても今後の設計において検討することになると認識。

山内構成員：タイムスタンプの検証に必要な情報はどのような情報であるべきかという点や、トラストリストの機械可読性などテクニカルな議論があったが、一般の方々にも分かりやすいように、一体誰が、何のために、タイムスタンプを検証したいのか、検証しなければならないのかという部分のストーリーについて、事務局を中心にまとめた方がよいと考えている。例えば、特許情報については、先発明主義の国々では様々な技術データがいつ作られたかが極めて重要になる。そういうものの電子データに対するタイムスタンプの検証は、一体誰が行うのか。検証者は必ずしも当事者とは限らない。第三者の場合もあり得る。リライングパーティが検証する場合に、それぞれのシーンにおいて、どのような人たちが、どういうニーズでタイムスタンプを検証するのかを分かりやすくストーリー化して、検証のための仕組みとして、このようなものが必要であるということを検討会の報告書にまとめることができれば、一般の方々にも分かりやすくなると考えている。

東條座長：その点はすごく重要。最終的に検討会の報告書という形で一般の方々に開示する際には、ビジネスに即して、誰が、何のために、どういうことを検証するのかという仕組みについての分かりやすい説明を心掛けてほしい。

小松構成員：証明書の検証は専用ソフトで自動的に読み込んでもらう形が必要ではないか。監査の観点でエビデンスが正しいものであるのかを判断しなければならないが、目視で判断が難しいと思われるため、サービスと一緒に専用ソフトが提供されなければ、有効性の確認が難しくなってしまう。例えば、SSL証明書の場合は、ブラウザベンダーが証明書の有効性検証機能をブラウザの中に取り込んでいる。そのような形でユーザーフレンドリーに専用の検証ソフトが提供されるとよい。

東條座長：重要な視点。この点は資料５－２の８ページで、今後丁寧に他のトラストリストも含めて、設計について検討していくことになっている。どれぐらいのタイムスパンでこれが実現されるのかという話とも関わると思う。

伊地知構成員：トラストリストの設計に関わるタイムスパンについては、今のところコメントはない。先ほどの御意見の中にあった専用ソフトというのは、検証する専用ソフトという理解でよいか。それとも監査業務の何か専

用ソフトになるのか。

小松構成員：両方のタイプがあると思う。監査の中で、エビデンスが正しいかどうかを検証できるように、専用ソフトを監査ツールの中に組み込めると望ましい。また、汎用的なソフトの中に組み込んでもらえるようになれば、一般の方々にも使ってもらえる。マイクロソフトのインターネットエクスプローラーやグーグルのクロームなどが、SSL証明書を自動的に読み込んで、いろいろと情報提供してくれる。そのようなレベル感での使いやすいソフトがあるとよい。

東條座長：続いて、事業体として求められる要件について、構成員の皆様の御意見を頂戴したい。

小田嶋構成員：資料５－２の14ページの事業体として求められる要件について、既存の制度も踏まえ、国の認定制度として整備するにあたっては、経済的基礎を求めることは適当であると考えている。

吉田構成員：欧州に見習って、事業の継続が困難であった場合に、代替事業者に確実に引き継いでもらえるような仕掛けがあるとよい。今回の認定制度の中にこのような仕掛けを入れてほしい。

伊地知構成員：EUでは、事業の継続が困難になった場合に代替事業者に引き継ぐ努力を定めている国もある。今回の認定制度の中でも、このようなことを定めるのが理想的ではあるが、日本データ通信協会の現行の認定制度の中ではこのようなことを定めていないのが実情である。

事務局：今指摘があった代替事業者への引き継ぎについては、資料５－１の１ページの「タイムスタンプ認定制度に関する検討会」論点全体像の中で、⑥その他の２つ目にある、廃業の場合の扱いの部分で改めて検討することになると考えている。

東條座長：本日議論いただいた２つの論点について、１つ目の認定業務の公表内容及び公表方法については、さまざまな御意見を頂戴した。いずれも重要な論点であると理解した。今後慎重に検討を行うことになるが、工夫が必要であるという印象を受けた。制度をスタートさせる際に、どういう内容で、どういう形式のものをトラストリストに掲載していくかという部分はもう少し議論を深めていく必要がある。今後も御意見を頂きながら検討を進めていきたい。

　２つ目の事業体として求められる要件については、日本データ通信協会の資料に記載されているとおり、経理的基礎を求め、なおかつそれを審査項目として規定することが適当ではないかという部分について構成員の皆様の共通の理解をいただいたという形で取りまとめさせていただきたい。

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