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）

１　日　時

令和２年７月１日（水）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、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、山本内閣府政策統括官（科学技術・イノベーション担当）付上席政策調査員、朝山法務省民事局商事課課長補佐、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

（ヒアリング対象者）アマノセキュアジャパン株式会社森口氏、上田氏、セイコーソリューションズ株式会社柴田氏、株式会社ＴＫＣ矢生氏、株式会社サイバーリンクス竹内氏、渋谷氏、三菱電機インフォメーションネットワーク株式会社渡辺氏、川崎氏

（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４－１　タイムスタンプ認定制度に関する検討会（第４回）事務局資料

資料４－２　日本データ通信協会提出資料

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）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４－１について事務局から、資料４－２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。

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構成員の皆様の御意見を頂戴したい。

宮崎構成員：資料４－２の１ページ目にある TSA 業務サーバーの機能について確認。外部からのリクエストの受付、レスポンスの発行や利用者認証等を行う等の機能を担っていると認識している。一般的には利用者が TSA 業務サーバーを介してタイムスタンプを取得することになると考えているが如何。

伊地知構成員：その認識で合っている。

梅本構成員：資料４－２の３ページ目に、今の TAA 方式では、時刻差証明書及びその発行記録の保存を求めており、運用規約上は 10 年以上保存するとある。では、仮にこの記録が 10 年以上経過して破棄された場合は、どの点が証明できなくなるのか。

伊地知構成員：タイムスタンプ自体の検証によって、データとタイムスタンプの結びつきや文書が改ざんされていないかどうか確認できる。タイムスタンプに使われていたデジタル署名が間違いなく TSA のものであるかどうかについては、認証局が発行している TSA 公開鍵証明書を検証することで、確認ができる。そして、タイムスタンプの時刻自体の正しさが議論になる場合、通常、そのタイムスタンプを利用する企業と係争になる相手方がいると想定される。TSA 自体が第三者であるため、そこまで深くは問われないと聞いているものの、TSA が時刻の正しさを証明するにあたり、TAA がさらなる第三者として時刻の監査を行い正しい時刻であると証明する時刻差証明書が用いられる。実際の係争で時刻差証明書が出された例は聞いたことはない。ただ、当該証明書は時刻のトレーサビリティという意味では、一番大本になるところの一つであり、厳重に保管しているのが実態である。

梅本構成員：仮に時刻差証明書が破棄されたとしても、TAA や TSA 自身の信頼性が高ければ、疑いが生じる可能性は低いということか。

伊地知構成員：第三者による時刻差の証明の必要性を判断するに当たっては、時刻の信頼性の証明が必要になる場合を残留のリスクとして飲み込めるのかどうかが非常に重要になる。そのため、技術的な話というよりは様々な分野で御経験、認識の深い方々の御意見を参考にしながら判断していきたい。

小松構成員：時刻差が原因となって、訴訟、重大事故や事件につながった例はあるか。

伊地知構成員：関知しているものはない。TSA の時刻の正しさが争点となり、それに関するエビデンスの提出が求められたケースについては、まだないと考えている。

東條座長：諸外国でも、法廷で争われたようなケースはないか。

伊地知構成員：中国やヨーロッパであったという情報はあるが、件数としてはあまり多くはないのが実情という認識。

吉田構成員：資料４－２の２ページ目に関連して、伊地知構成員の説明はあくまで適格トラストサービスプロバイダー（以下、「QTSP」という。）がどうあるべきかという話だと認識。恐らく EU では QTSP ではないトラストサービスプロバイダー（以下、「TSP」という。）は、NTP をそのまま引っ張っているような形になっている。そのため、我が国のタイムスタンプの認定に当たり、複数のソースを提示いただいたのは適切で、複数用いることを指針に入れるべき。GPS は 2000 年の頃の太陽風のロールオーバー問題など、良くない点もあると思うので、ソースは３つ必要といったことを盛り込む必要もあるのでは。

事務局：メインの時刻源をどうするか、そして、チェック用の時刻源を設ける必要があるという御意見と認識。それは信頼の確保の仕方として確実な方法だと思う。資料４－２の２ページ目に様々な時刻源も提示している。他の構成員の方からも意見を伺いたい。

伊地知構成員：タイムビジネスの認定に関わっていると安全性の観点からしっかりした時刻源を選ぼうという気持ちが非常に強くなる。そのため、多くの皆様の御意見を聞いた上でどのような基準が適切かを議論し、決定するのが妥当。

東條座長：中国は時刻源が１つの場合もあり得るというお話を前回御紹介いただいたが、ヨーロッパは基本的には２つでやっているということか。

伊地知構成員：EU については、９社の運用規程を調べて、公開 NTP だけを使うところが２社、GPS、GNSS だけを使うところが２社、残り５社はその両方を用いているというように前回の資料３－２でまとめさせて

いただいた。公開NTPだけの２社については、GPS等何も使わずに公開NTPだけでやっているという可能性もある。ただ、公開NTPのみであっても複数のNTPサーバーを参照して運用すれば、極端に狂った時刻にはならないと認識している。一方で、現在日本でやっているように、TAAの時刻、UTC（NICT）に至るところまでしっかり全ての証拠を残すという観点でいくと、公開NTPだけを用いる場合はインターネットの先にあるサーバーに時刻を合わせただけなので時刻の信頼性を証明し切るのは非常に難しい。

東條座長：制度普及の観点から２つの時刻源を参照するとコストが跳ね上がるということはないか。

伊地知構成員：時刻源をどのように選び、どう組み合わせるかによって費用は変わる。

岩間構成員：資料４－２の２ページ目の一番上の時刻情報提供サービスはNTPサービスだが、専用線でつなぐという形であり、現行のタイムスタンプサーバーと非常に親和性が高いサービスとなっている。そのため、専用線の費用はかかるが通常のNTPと同じような形で使うことができ、完全にピア２ピアでつながる。もう一つの光テレホンJJYは電話回線を使うということで、時刻情報提供サービスと同じく、NICTとのトレーサビリティが取りやすいが、受話装置が必要になってくるという点で違いがある。いずれもNICTとダイレクトにつながっているため監査しやすい。NICTで公開NTPもやっているが、商用で使うのであれば、上の２つは非常に使いやすい。

　もう一点、GPS、GNSSについてだが、ヨーロッパではガリレオという衛星を自ら扱っておりEUの時刻という形で捉えられる。中国でも北斗という、国の事業であるGNSSを使っているため信頼できる時刻となっている。しかし、ITUの申合せでSAというGPSの精度を極端に落とす作業は行わないことになっているが、GPSは米軍のシステムであり有事で必要な際はSAをかける可能性があるため、日本の場合、GPS一本で行くというのはちょっと厳しい。

吉田構成員：ソースを増やせば時刻の信頼性は高くなるが、コスト、資格、メンテナンス、監査等が増える結果、アプリケーションベンダーやプロバイダーに使われなくなり、EUのようにQualifiedではないTSPが多数成立する可能性もある。今回はQTSPであるため、使うべきソースを明示しなければコストや浸透の観点で問題があるだろう。

伊地知構成員：時刻情報提供サービスは専用線ではなくても大丈夫というような理解でよろしいか。専用線を用いたサービスを使うとなると、

NICT 側、事業者側の回線も費用負担が発生するため、月額それなりの費用がかかるのではないか。専用線以外にもう少し廉価な接続方法はあるか。

岩間構成員：専用線を維持するというのはコストがある程度かかるかもしれないが、ひかり電話の電話網を使う光テレホン JJY であればそれよりは安く、ミリ秒以下の精度で時刻を取得できる。

東條座長：続いて TSA 事業者の皆様から意見を頂戴したい。

上田氏：タイムスタンプ自体の時刻源としては、UTC(k)を使うことが世界的な流れだと思うので、日本の場合は UTC(NICT)を利用することが適切ではないか。

タイムスタンプ発行前の時刻精度確認については、タイムスタンプサーバーからその時刻源である NICT のサーバーまでの経路上の機器や通信回線に障害等が起こり得るという可能性を踏まえると、異なる時刻源、UTC(NICT)以外の時刻源を使ったチェック機構が必要と認識。そして、異なる時刻源は GPS、GNSS 等の衛星を使った時刻を使用するのが現実的ではないか。

時刻のトレーサビリティとしては、TAA を使わない運用となるため、当然タイムスタンプサーバーやタイムサーバーといった各機器における上位の NTP サーバーとの時刻同期のログ、すなわちタイムスタンプサーバーで言うとタイムサーバーとの同期のログ、タイムサーバーにおいて言うと、UTC(NICT)との同期のログ、これらをしっかり保存して、開示できるようにしておく必要がある。

柴田氏：タイムスタンプにおいて最も重要な時刻の信頼性を TSA 自ら証明するとなると、自分で自分を証明する形になるため、どう信頼性を担保するかというのをよく考える必要がある。そのためには、自走しているタイムスタンプサーバーの時計でタイムスタンプが押されていることを、どう証明するか考える必要があり、結局タイムスタンプサーバーのログをどのように確保するかが重要になる。ログ等の情報を保持すべき期間としては、基本的にタイムスタンプそのものの有効期限は 11 年であることを踏まえ、少なくともそれ以上ということになるだろう。ログをどのように持つかということを議論するべき。

時刻源は NICT の時刻源がいいと考える。国家の認定である日本標準時に準拠するべき。また、タイムスタンプとして外へ出すときに、その時刻は正しかったか確認する必要があるため、別の時刻源、具体的には GPS でもって、チェックするという考え方は適切。現状もそうした仕組みになっているので事業者としてもありがたい。

渋谷氏：時刻源についてはNICTから取るというのがいいと思っている。また、時刻のトレーサビリティを確保することは重要だとは思うものの、このログは正しいというのをTSAだけで証明するのはなかなか大変だと思う。どういう形で表現したら、正しい真正性のあるデータだというのが証明できるのかを考えていきたい。

川崎氏：時刻源についてはNICTが提供する時刻源を使うのが望ましい。

時刻精度の確認としても複数の時刻源でチェックする必要があると思う。この場合、例えば有線で取るものと無線で取るものというように経路も含めて複数の時刻源から取るのがよい。有線でも、道路工事等により通信回線の障害が発生し得るため複数の経路を取ったほうがよい。

時刻のトレーサビリティについては、TSAのタイムスタンプサーバー自身でログをしっかり取って、ログを改ざんされないようにする必要がある。タイムスタンプサーバーをどういうふうに実装していくかというのは今後の課題だろう。

宮崎構成員：厳密で安全で非改ざんであるログを確保するにあたり、ログのレコード間でハッシュのリンクを取ることで改ざんを検知するやり方もある。しかし、このやり方をとるとリンキング方式のタイムスタンプと同じような形になり、これまで発行した全てのタイムスタンプについてハッシュのリンクをつなげていく必要が生じ、運用コストもかかり検証も大変になる。ログの安全性確保という意味で何らかの工夫をする必要があるが10～11年を経たある時点で、それまでは不正がなかったことを確定できるような何らかの仕組みが必要。また、TSAが自ら保証する方式でやっているヨーロッパの相場観も調査する必要がある。

上原構成員：トレーサビリティの確保のためにログを保存するという考え方には賛同。特許等でどちらが先にデータを取って確定していたのかというところが議論になった場合は、ログを証拠として提出することになると思う。製薬会社の場合は特許が切れるぎりぎりで争うため、10年以上の非常に長い期間のログが欲しいという話になる。ただ、使うかも分からないデータをすぐに生かせる形で取っておくことはコストもかかるため、例えば、電子データをまとめてZIPファイルにしてタイムスタンプを押して保存しておき、使うときはそこからコピーして使うといった方法もあると思っている。

伊地知構成員：現行制度の保存期間について、事業者が決めている10年を非常に長いと感じる方もいれば、例えば製薬では20年間が一般で

あって 10 年では足りないといった意見もある。利用場面によって、求められる期間も変わってくると思う。そういった様々なニーズに対応できる仕組みが作れると、一番よいと思うが今の段階では具体的なアイデアは持ち合わせていない。

東條座長：続いて、認定の期間（認定の有効期間）についての意見交換をお願いしたい。

上原構成員：現行の制度について確認したい。更新審査のときに不適合事項が発見された場合はどうなるのか。

伊地知構成員：信頼性に影響を及ぼしそうな事態が生じた場合にはまず調査をし、その結果により立入調査も行い、場合によっては業務の改善要請をして、最後には認定の取消しをするというような制度上の建て付けはできている。また、実際に認定の更新の審査の際に不適合があったケースとして、資料の更新が遅れていた等の軽微なものはあるが、タイムスタンプの信頼性に影響を及ぼすような大きな事案というのは、少なくとも私が見ているこの５年間においてはない。過去ももちろんなかったのではないか。

西山構成員：認定の有効期間について。EU の制度では認定の有効期間が２年で回っているが、日本では、タイムスタンプ局は毎年鍵更新をする。鍵更新をした後の鍵の確認をどのようにするかが重要であり、２年という結論にすぐ飛びつくのは危険。現行の日本の制度では、鍵更新時に現地の立入検査のようなことはやっていないという話だが、鍵更新の報告について立入りまではやらなくても、それを二重にチェックができるような何らかの方式について検討は必要ではないか。EU では、どのように認定の有効期間を２年で回しているのかという情報があればありがたい。

柿崎座長代理：鍵の更新のタイミングは非常に重要だと認識。認定の期間を鍵更新のタイミングにあわせるというのも一つの手だとは思う。ただ、EU との適合性を考えたときには、２年という考え方が多分一番なじむのではないか。

伊地知構成員：EU では、５年間の有効期間を持った証明書を用いてタイムスタンプを発行し、その中間にあたる２年半で鍵を更新するような措置を取っている例もある。鍵の更新に関する考え方が、日本と EU では大きく違うと思う。日本は１年ごとの定期的な更新に加え、ハードウエア・セキュリティ・モジュールのトラブルや障害などが発生した場合等、臨時で鍵の生成をするといったこともあるため、頻度が高まる。一方で、どういう鍵を生成したのか、TSA をきっちりと押さえる

ことは極めて重要。ここについては認定の更新とは別に確認する方法というものを技術的に確立していく必要がある。

小田嶋構成員：現行の２年に関してはEUとも同じなので、特に反対はない。毎年行っているTSAの鍵更新はトラストの基盤になるもの。例えば、電子署名法における変更認定のような扱いで、２年のうち１年は鍵更新に係る部分だけを調査するということも考えられるのではないか。また、TSA公開鍵証明書についてはトラステッドリストに掲載されることになると考えている。

宮崎構成員：現行では、有効期間２年の認定制度で問題は生じていないとあるが、それは業務を特定するための識別子となる公開鍵証明書が考慮されていないためである。EUでは認定対象の業務を一意に特定するためにその業務が用いる公開鍵証明書を業務の識別子として用いる。これをデジタルＩＤと呼ぶが、それをXMLで記述された機械可読のトラステッドリストに含め、検証ソフトがデジタルＩＤをトラストアンカとして利用する。EUが有効期間２年で問題ないのは、EUでは公開鍵証明書を毎年更新する運用をしていないため、２年に１回の認定で、そのデジタルＩＤであるTSAの公開鍵証明書がしっかりとチェックでき、トラステッドリストに入れられるからである。

　一方、現行では国内のTSAは毎年鍵更新を行い公開鍵証明書も毎年更新されるが、今後、公開鍵証明書更新に関してチェックしなくてはならなくなるということを踏まえると、毎年監査を行う、鍵の使用期間を２年に延ばす、あるいは中間の１年目には鍵の更新に関する部分だけを監査するといった何らかの対処を行う必要がある。これについては後々の論点⑤の認定業務の公表内容及び公表方法と併せて検討しなければならない。

山内構成員：認定の有効期間について、ISMS適合性評価制度の認定機関及び電子署名法に基づく指定調査機関の観点でコメント。認定の有効期間の選択肢で、３年（ISMS）との記載については、事実関係からすると少し不足している。まずISMSについては、認定ではなく認証という言葉が適切。ISMSの認証機関が組織を認証するにあたっては、初回の認証から３年経った時点で更新するが、それまでの間の１年目、２年目にサーベイランスを行い、認証を維持している。審査の費用の大きさのイメージは、初回の審査が「３」、３年後の更新審査が「２」、１年後と２年後のサーベイランスが「１」である。つまり、ISMS認証において、更新審査の間隔が長いからといって、必ずしも事業者の負担が軽減されているわけではない。毎年認証機関が組織に出向き、

ISMS という情報セキュリティマネジメントシステムがしっかり運用されているかを確認して認証を維持していることをご理解頂きたい。

次に、電子署名法に基づく特定認証業務の認定に係る調査については、認定の有効期間が１年のために更新調査に係る事業者及び指定調査機関の負担が大きいということではない。経済産業省の電子署名法研究会で詳細な議論をした結果、１年毎の更新でも負担が少ないような形になった。

個人的に、タイムスタンプの認定については、鍵の更新の部分に、ISMS 認証のようなサーベイランスという概念を入れてもいいのではないかと思っている。

東條座長：最後の論点、調査機関の要件について御意見をいただきたい。

宮崎構成員：資料４－２、６ページの調査機関の指定の基準について。国際通用性というのを考えた場合は、指定の基準を国際標準に準拠するような形にする必要がある。７ページに EU における認定の仕組みとあり、EN 319 403 に並んで ISO/IEC17065 とある。基本的にその ISO/IEC17065 というのが、調査機関の認定の基準のようなことが記載されている国際標準で、様々な制度でこれを利用して認定を行っている。それに対して EN 319 403 というのは、それを TSP 向けに変えた場合の差分について基準を示したヨーロッパの標準になっている。ISO は JIS にもなっていて、具体的には JISQ 17065 になっている。指定にしても認定を行うにしても、基準を作り、その際には ISO や JIS をベースに EN 319 403 のような考え方で、タイムスタンプであればタイムスタンプに特有の差分を改めて定義していくという形でやっていくのがいいと思う。

伊地知構成員：仮に指定のような方式を取るとしても、指定に関する要件については、今の電子署名法のような定め方ではなく、EU の EN 403 や ISO 17065 といったものに準拠できるような形で規定をすべきという指摘だと理解。こういった制度を作るための仕組みについて、どのように、どこで定めていくかは非常に難しい問題。

西山構成員：宮崎構成員の意見に対する賛成のコメント。電子署名法の第 20 条では４項目程度しか項目がない。それに対して EN 319 403 では、項目数としては 60 前後あり、粒度が全く異なる。国際的な相互承認という観点でいくと電子署名法は問題があると思う。それから今後、ｅシールの認定はもちろん、リモート署名の認定の検討をする機会もあるという可能性を踏まえると、それぞれのトラストサービスの適合性評価をどういった方々にやっていただくのが適切かということ

をしっかりと検討しておく必要があると思う。ISO 17065 に加えて、TSP の調査における特異的な要件を追加した EN 319 403 のようなものの検討は必要ではないか。

事務局：EN 及び ISO に規定する基準をどこまで踏まえる必要があるかということについてトラストサービス提供事業者を含め、よく相談して検討する必要がある。

上原構成員：製薬業界では、製造や安全性の試験などをしている場所や製造場所について当局から監査を受け、企業同士で監査を受けた機関であることを認め合う必要がある。その際、監査機関の基準がグローバルでそろっているとお互いに受け入れやすい。調査機関の要件に関する論点についても似たような考え方だと感じている。ISO/IEC と書いてある部分を共通の基礎にした上で各国の特徴を踏まえ、差分を受け入れていくという方向性には賛成。

吉田構成員：各業種への対応と使い勝手はトレードオフだろう。例えば EN 319 403 に定義されていない EU の世界で言うと、事業者が潰れた場合に政府がその事業を継続するといったたぐいのものがある。そのため EN に定義されていない部分の定義も我が国として持っておく必要があると思う。

東條座長：本日の取りまとめをさせていただく。第１の TSA が自ら時刻の信頼性を確保する方式については、具体的な時刻源、時刻の同期精度、トレーサビリティの確保の仕組み等について、諸外国の実態をもう少し情報収集して整理しつつ次回以降引き続き議論をいただきたい。

第２の論点、認定の期間だが、これは EU の制度に合わせて２年でも構わないという意見が多く、反対意見は特になかったように承った。ただ、具体的な論点については制度の設計を工夫する必要があるということも確認されたところ、ベースは２年ということで、さらに議論を深めてまいりたい。

第３の調査機関の要件については、EU の制度といった国際的な制度との整合性という観点の重要性にも鑑み、本日の議論を基に、事務局にて整理をいただきたい。

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