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）

## １　日　時

令和２年 10 月 20 日（火）10:00～11:15

## 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、萩原氏（山内構成員代理）、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）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

（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７－１　タイムスタンプ認定制度に関する検討会（第７回）事務局資料
資料７－２　日本データ通信協会提出資料
参考資料７－１　データ戦略タスクフォースの開催について
参考資料７－２　調査を委託する機関に求められる要件（再掲）
参考資料７－３　トラストリストへの記載事項等（再掲）
参考資料７－４　廃止の場合の取扱い（再掲）
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)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７－１について事務局から、資料７－２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：まずは、調査・監査の内容について意見交換をお願いしたい。

宮崎構成員：資料７－２の３ページに、日本の調査・監査と、EUのフル監査・サーベイランス監査が記載されているが、それらの対応関係について教えてほしい。

伊地知構成員：日本の認定及び更新に係る調査は２年に１回実施している。EUでこれに該当するのはフル監査で、同じく２年に１回実施している。日本の認定期間中に実施する監査は内部監査でも可能になっており、１年に１回実施している。EUでこれに該当するのはサーベイランス監査で、２年に１回実施している。EUの内部監査について、情報をお持ちであれば説明してほしい。

宮崎構成員：EUでは、１年に１回内部監査を実施している。２年間という期間で見た場合には、日本では、調査を１回、監査を２回、計３回の調査・監査を実施している。他方、EUでは、フル監査を１回、サーベイランス監査を１回、内部監査を２回、計４回の調査・監査を実施している。この日本とEUの回数の違いは意識して検討した方がよい。

東條座長：日本とEUの制度には違いがあるが、今提案されている制度でも調査・監査の頻度は十分であるという意見でよいか。

宮崎構成員：タイムスタンプについては、国際的な通用性が重視されるが、日本とEUでは調査・監査の回数に差があることは意識して、EUと交渉する必要がある。場合によっては、日本の３回の調査・監査は不十分であると思われる可能性がある。日本として、それでも十分であると説明する場合はしっかりと理由を考えておくべきである。

東條座長：EUとの交渉次第になるが、仮に監査の追加を求められるとすれば、例えば、サーベイランス監査のようなものを追加することになるか。

宮崎構成員：多分そのようになると思う。ただし、サーベイランス監査はフル監査の50%程度しか実施しないため、その部分は調査と同じ内容を実施する日本の内部監査でカバーできているから大丈夫であるという主張ができるかもしれない。

上原構成員：日本とEUの基準の差が大きいことで国際的な通用性に関する交渉に時間がかかるのであれば、タイムスタンプを活用する側として利用を勧

めにくい。できるだけ日本とEUで方向性を合わせて頂きたい。

西山構成員：国際通用性に関する議論は、監査以外の論点も含め総合的に交渉されるのではないか。

宮崎構成員：資料７－２の１ページ目に、ハッシュ関数の脆弱化、TSA公開鍵証明書を発行する認証事業者の廃業等、必要に応じ都度対応してきているという記載があるが、この対応で十分か。何らかの規定を設けるべきではないかと思う。日本データ通信協会では、どのように考えているか。

伊地知構成員：審査基準については、制度が始まって間もないタイミングでハッシュ関数SHA-1の脆弱化に対応したことに始まり、この15年間に10回程度改正している。先ほどの規定を設けるべきという意見は、見直しのサイクルの仕組みを何か作るべきという意見であると承知しているが妥当だと思う。

宮崎構成員：何らかの規則、ルールがないと、場合によっては見落としてしまったり、必要性を感じなくなったりするなど、様々な不都合が生じるのではないかと思う。そのあたりについては、何らかの規則、ルールを考えておくべきである。

東條座長：アドホックに対応するのではなく、きちんと定期的な見直しを行うということを内規などで定めるというイメージになるか。

伊地知構成員：審査基準のメンテナンスについて、どのような体制で、どこが責任を持って実施するのかということについても、これからの調整事項であると認識している。日本データ通信協会が関与できる場合には、きちんとメンテナンスのサイクルについて議論して決めるのが妥当ではないかと認識している。

梅本構成員：資料７－２の２ページ目に、現行制度にはない新たな観点として、事業体として求められる要件に、経理的基礎が追加されている。最も単純な基準としては、資本金額等が考えられる。しかし、この要件は事業の継続性を裏付けるためのものなので、例えば既に他の事業を展開しているような事業者については、他の事業の状況などを判断要素に含めるなど、ある程度総合的に、かつ柔軟に判断できるようにした方がよい。

伊地知構成員：ご指摘を踏まえて、今後、総務省の委託事業を通じて、野村総合研究所が事務局となって行う、基準に関する議論の場等を踏まえて判断していくべきであると認識している。

東條座長：次にTSA公開鍵証明書を発行する認証事業者の基準について意見交換をお願いしたい。

宮崎構成員：資料７－２の６ページに、認証事業者の基準について記載されている。実際の調査では、認証事業者を調査することが難しいという話が出

たが、例えば、使っている暗号アルゴリズムや証明書に規定すべき値やプロファイル等について、時刻認証局（TSA）から認証事業者に対して、最低限確認したり要求したりすることを規定することは考えられるのではないかと思う。この他に重要なものとして、失効させる場合の理由のコードがあるが、それについては、TSA側が、認証事業者に対して確認、要求すべきことを規定するという何らかのスキームができるのではないか。

伊地知構成員：来年４月に制度を始める段階では、事業者として考えて判断するしかないのではないかと考えている。将来的には、EUのようにあらゆる業務について、共通の仕組みで適格性が認められるようになれば、制度として運用しやすくなるのではないかと考えている。

西山構成員：来年４月に始まる制度ということが前提であっても、TSAから認証事業者に対して、ある程度要件を提示することによって、ある程度信頼の置ける認証事業者を選定することはできるのではないか。その基準をブレイクダウンして作成することは、実務的に可能であると思う。

国際通用性の観点に立てば、EUの場合、認証事業者は適格認証事業者であることが要求されているため、そうなるとそもそも認定認証業務がEUの適格に該当するかどうかの確認が出来ていない状態であるため、議論に少し時間がかかると思う。ただし、将来的には、そのような方向性も考えざるを得ないのではないかという気がする。

認証事業者のなりすましの観点については、トラストアンカーの公開という形で何らかの適切な適格認証事業者を公開することをセットで考える必要があると思う。日本データ通信協会の制度では、ルール上、認定認証事業者と同等であることか、WebTrust監査を受けていることの２つが想定されているが、WebTrust監査と同等なレベルとして、ETSIの監査基準による監査があるので、それについても考えられるのではないかと思う。

伊地知構成員：認証事業者に関する要件について、TSAに対して求めるという方法は考えられると思う。例えば、現状では、認証事業者が認定の時刻認証業務にしか証明書を出さないといった部分について特段の定めをまだ行っていない。そのような部分を改良出来れば、EUの適格認証事業者のような形で、適格認証事業者の証明書だけでしっかりとした把握がしやすくなる状況を作ることができると思う。

東條座長：来年４月からキックオフするための短期的な対応と、その後見直しをしていくという少し長いスパンでの対応を意識的に区別しながら議論を進めていってほしい。

山内構成員代理（萩原）：資料７－２の６ページに、実際に利用されている認証事業者が記載されている。電子署名法の認定認証事業者、認定認証業務

が該当すると思うが、基本的にGMOグローバルサインは、EUの適格認証事業者であり、eIDASの認定を取得しているTSAや電子署名の証明書の認証業務でもあるので、適格を取得している認証事業者も１つの参考になるのではないかと思う。

伊地知構成員：EUの適格認証事業者について記載していないのは、日本データ通信協会の制度の基準では、EUの適格認証事業者を対象にしていないからである。今回の制度でEUの適格認証事業者やETSIの認定を対象にすることについては、国際相互承認の将来的な交渉にも影響するような要素でもあることを認識しながら、いろいろと議論する必要があるのではないかと考えている。

事務局：資料７－２の６ページに、審査基準を抜粋しており、信頼のある監査機関のエビデンスの例として、WebTrustを明記している。GMOグローバルサインはWebTrustの認定を取得していて、子会社がベルギーに認証事業者を持っている。そこがEUの認定を取得しているという認識である。たまたまEUの基準も満たしているが、EUの基準でここまで幅広く議論してきた訳ではない。WebTrustプラスアルファで信頼性を高めるものとして参考にはなるかもしれない。

西山構成員： GMOグローバルサインの本社は日本であるが、認証事業者はベルギーの認証事業者である。従って、EUの認証事業者と捉えた場合には、それこそいっぱいあるので、それを一々判断するのはなかなか難しいのではないかと考えている。

東條座長：EUの適格認証事業者を対象にするかどうかという点については、将来的に別途検討が必要であるという整理でよろしいか。

小松構成員：GMOグローバルサインは、EUの制度を取得しているが、制度に関しては日本での認知度はまだ低く、どのような形で監査を受けているのかはよく知られていない。一方、WebTrustについては、日本公認会計士協会でWebTrust保証業務が認知されており、実務指針もきちんと作成され、広く一般に公表されている。その中で実務が提供されているので、日本の制度として定着している。そのような差があるので、EUの制度を導入するのであれば、日本で周知したうえで導入するという形が望ましいと思う。

山内構成員代理（萩原）：先ほどの発言に補足する。実際に利用されている認証事業者の例に、WebTrustという業界基準が入っているので、eIDASの認定事業者も参考情報として資料に記載してはどうかという趣旨で発言した。

東條座長：それではこれまでご議論いただいた論点についての議論をお願いしたい。

小田嶋構成員：資料７－１の８ページ目について、事務局の見解として、過去の履歴情報もあわせて公開することが有用という記載があるが、この過去の履歴情報について、どの時点をポイントにするか。例えば、来年４月から開始されるということであれば、来年４月からにするのか、過去のタイムスタンプが開始された時点からにするのか。一旦何らかの決めが必要になるのではないかと思う。

伊地知構成員：来年４月のスタート時点では、トラストリストを本格的に運用する訳ではなく、総務省のホームページに公開鍵証明書などを公開する方向になっていると思う。他方、現行の制度は民間の認定制度であるので、公開する場合には明確に新しい国の認定のものと識別できる形で掲載する必要がある。過去のものの掲載に関しては、このような工夫をしながら、もう少し今後のトラストリストの設計等の中で丁寧な議論を行いながら進めていくことになると認識している。

西山構成員：仮に総務省のホームページでTSA公開鍵等を公開することになる場合、トラストアンカーの真正性の確保が重要になる。例えば、認定認証業務では官報に認定認証事業者や公開鍵証明書のハッシュ値を公開しているが、インターネット官報等で電子的に官報を見ると、国立印刷局のeシールが付与されることによって、インターネット官報の真正性が担保されている。そこで公開された認定認証事業者のハッシュ値というのは非改ざん性を確保、改ざん検知機能が担保されている状況になっている。従ってトラストアンカーを公開する際には、ぜひ官報のようにeシール等を付与して真正性を担保することについて検討してもらいたい。

事務局：TSA公開鍵証明書を総務省ホームページに掲載するということは案の１つとして考えており、具体的にどのように実施していくのかは今後検討しなければならない。例えば、事業者から提供されるTSA公開鍵証明書に総務省の官職証明書による電子署名を付けて総務省ホームページに掲載することはあるかもしれない。eシールに近い仕組み等を活用することも考えられると思う。小田嶋構成員から話のあった過去の履歴情報については、来年４月以降、短期的に始められることと、長期的な視点で検討することのうち、どちらかと言うと後者となり、長期的に検討されるトラストリストになると考えられる。

宮崎構成員：廃止に関わる終了届や終了計画について、確かに事業者に過度な負担を与えたり、利用者に過剰な信頼を与えたりすることはなるべく避けたいところである。ただし、突然タイムスタンプの有効性が失われたり、発行済タイムスタンプが偽造されたりする状態になることは一番避けなければならないことである。この部分を如何に防ぐかという観点から、最

低限必要な終了計画や予め実施すべき措置を検討することができればよいと考えている。

伊地知構成員：タイムスタンプが一旦効力を失ってしまうと、それを改めて証明するということは実質的に不可能であると考えられることから、そのような事態が生じないようにきちんと終了計画を定める。この終了計画については、EUの場合、ENISAがガイドラインを公表しており、その中でどのようなことを定めるべきか、ということが示されている。日本でもトラストサービス推進フォーラム等で議論を行いながら、そのようなガイドラインを少しずつ整えていくことが必要ではないかと思う。

柿崎構成員：資料７－１の９ページに、業務廃止に際し、利用者に余裕をもって廃止の旨及びその終了計画を通知することを規定することが適切と記載されているが、これをどこに通知するのか。トラストリストに、このタイムスタンプはいつから廃止が計画されているという情報を掲載して公開し、それを検証しようとする利用者や機械が、それを認識して、そのタイムスタンプがいつから発行されてはいけないものであるかを確認できるようにする必要がある。廃止計画と廃止の届出が公開されることが重要ではないかと考えている。

伊地知構成員：トラストリストができた場合、その中できちんと認定された機関がいつ廃止になるかという情報が予め分かるようにすることが理想と認識。これについても、トラストリストの設計の中で長期的に取り組んでいく必要がある。

小田嶋構成員：資料７－１の９ページについて、利用者に余裕をもって廃止の旨及びその終了計画を通知することが記載されているが、利用者に余裕をもってという表現では少し曖昧ではないかと思う。少なくとも例えば、３か月前、４か月前といったある程度基準を設けた方がよい。電子署名法の場合、認定に関わる指針の第十二条の第二項で60日前ということが定められ、利用者に通知することになっている。同じように数字で示して記載した方がよいと思う。

伊地知構成員：現行の制度では、各事業者が運用規程の中で廃止する場合の通知等を規定している。３か月前を目安にしていた。先ほどの意見を踏まえて議論することが必要であると認識した。

事務局：例えば、３か月前等、そのようなものを念頭に置いていたが、60日前も参考になる数字ではないかと考えている。

宮崎構成員：資料７－１の８ページに記載されているが、これまでもヒューマンリーダブルな形式、マシンリーダブルな形式ということでトラストリストについて議論してきたが、マシンリーダブルな形式はヨーロッパでは必

須になっている。これは検証のために使うためということもあるが、ヨーロッパではトラストリストブラウザというツールが提供されており、マシンリーダブルな形式のトラストリストをヒューマンリーダブルな形式で表示するツールがある。そのようなツールがあるので、わざわざヒューマンリーダブルな形式のトラストリストを検討する必要はない。そのために、ヨーロッパでもヒューマンリーダブルな形式の方はオプションになっている。そのあたりの状況を確認してほしい。

東條座長：これについても、来年４月からの規定の改正にあたっての短期的な視点と、それから先の長期的に取り組むべき視点という区別を持って整理をさせていただく。

事務局：マシンリーダブルは確かに便利であると思うが、そもそもヒューマンリーダブルなトラストリストもまだないので、先ずはそれを来年度以降に作成していく。それ以降の長期的な視点として、マシンリーダブルや過去の履歴情報の公開といったことを考えていくことが必要ではないかと考えている。

東條座長：調査・監査の内容については、資料７－２の４ページに記載されているとおり、現行制度における５つの観点に加えて、事業体の要件を追加することで十分である。内部監査でも可とする今回の制度においては、監査は全項目実施することが適当であるということで取りまとめをさせていただく。それから、国際通用性の観点からの意見をしっかりと確認したうえで、そのような観点に配慮しながら、制度を作っていくということでお願いしたい。

TSA公開鍵証明書を発行する認証事業者の基準については、TSAが認証事業者を選定、判断できるように、認証事業者の基準を明確にすることが適切である。そのときの基準は現行の制度からのシームレスな移行を考慮し、電子署名法の認定認証事業者やWebTrustに適合した認証事業者であることを求めることが適当であるということで取りまとめをさせていただく。

これまでに議論いただいた３つの論点については、資料７－１に列挙されているような見解で異論はないということで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