参考資料３－１

タイムスタンプ認定制度に関する検討会（第２回）

１　日　時

令和２年５月１日（金）

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）朝山法務省民事局商事課課長補佐、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）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、小高行政管理局行政情報システム課情報システム管理室室長

４　配付資料

資料２－１　事務局説明資料

資料２－２　日本データ通信協会提出資料

参考資料２－１　タイムスタンプ認定制度に関する検討会（第１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

事務局から参考資料２－１に基づき、前回会合の振り返りが行われた。

②　タイムスタンプ認定制度に係る認定の基準について

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

③　意見交換

事務局説明の後、意見交換が行われた。主な意見等は次のとおり。

東條座長：まず第１の論点である認定の単位について意見をお願いしたい。

宮崎構成員：今後の議論においても重要なため確認するが、「認定：accreditation」や「認証：certification」という言葉は、ＩＳＯ／ＩＥＣ１７０００とかＪＩＳＱ１７０００に用語や一般原則ということで定義されているもの。

資料２－２の「認定」という記載は、後者を意味する内容であり、ＪＩＳでは「認証： certification」と訳されるもの。本来の意味では、「認定：accreditation」というのは、認証機関やトラストサービスプロバイダを評価・監査する適合性評価機関等に関して、特定の適合性評価業務を行う「能力」や「適性」を持っているということを判断した上で、当該業務を実施してもよいということを認める、といった文脈で使用する用語。そのため、電子署名法やデータ通信協会のタイムビジネス認定制度においても同様だが、今回議論を行う「認定の対象」の「認定」は、本来は、製品やプロセス等に関する第三者証明を意味する「認証：certification」と呼ばれるものである。

ただし、今後、本検討会の議論の中で「認定」といっているのを「認証：certification」と言い換えるかどうかということについては、これまで「認定」という言葉を使っているので、このままでいいとは思うが、場合によっては混乱が生じることも想定されるので、そのときには一応確認して、しっかりと使い分けをするべきだろう

また、認定の単位を業務にすることは賛成。EU の eIDAS 規則や我が国の電子署名法も同様である。その一方で、認定された業務を、どういった手法で、機械的に一意に特定するのかが論点となる。電子署名法でも、認定された業務で用いるルート証明書のフィンガープリントを官報に載せており、それと照合することによって、確かに当該業務が認定を受けたものかどうかということが分かるという仕組み。タイムスタンプについても同様の仕組みが必要ではないか。

事務局：ご指摘に留意をして、今後の議論を進めていきたい。

伊地知構成員：認定の対象となる業務を機械的に一意に識別できる必要があるということについては、認定の公表に関する論点のところで、例えばＴＳＡの公開鍵証明書を特定して WEB ページに掲載するといったようなことなどが考えられる。

小田嶋構成員：業務の特定については、ＴＳＡの公開鍵証明書を特定するということだと思っている。電子署名法では、他の業務と誤認を防止するといった観点から指針の第１０条の２号、指定調査機関の調査に関する方針第４の９番目に記載がある。

　また、業務を特定する手段として、事業者がサービスのポリシーを定めて公表している運用規程において、業務の特定が可能となる内容の記載が必要ではないか。

梅本構成員：運用規程の書き方が事業者によって異なることもあると思う。あらかじめ識別する要素を示し、ある程度運用規程や利用規程が定型的な書き方ができるように例示をするなどしたほうがいい。その方が利用者への情報提供にもなり、各社のサービスの比較もしやすくなる。

伊地知構成員：現在、事業者の運用規程については、比較的似たようなつくりになっており、分かりにくい部分は少ないと思う。しかし、ガイドラインなどを示すことで定型化していくということが必要。

　また、実際の運用規程の中に、現在でも例えばサービスタイプ等様々な記載において、異なる概念を包含した記載となっているケースがある。その中に認定対象のサービスとそうでないものが混在しているというようなケース等については、十分に検討する必要があると認識。

若目田構成員：そもそも、今回認定制度を作ることになったのは何らかの課題があったからであり、認定の単位についてもその課題にフィットしているかどうかという観点で考える必要があるのではないか。情報銀行の認定制度検討の際にも、同様の論点が議論された。例えば、事業者全体の認定とした場合は、財務的な安定性なども対象となるため、信頼感につながるという利点があるが、業務単位の認定という選択肢も残さなければ、安全管理措置などについて事業と直接的な関係がないところも含めて全て評価する必要が生じ、ロスが大きいという指摘もあった。現在の認証制度の課題を踏まえ、それぞれのメリット、デメリットについてどう考えるか。

伊地知構成員：現状の制度が事業者単位になっていることについては、デメリットがあるということを認識しており、業務単位ということを中心に検討した。一方で、業務単位の場合のデメリットは、認定の対象が何なのかということを明確に特定することが非常に難しいということ。

　ＥＵのように、サービスを認定しつつも、事業者についても認定事業者と呼ぶような概念もあるのではないか。さらには、認定のタイムスタンプかどうかを判定するための公開鍵証明書などの特定ということも必要。

吉田構成員：この論点は総論としては賛成。事業者としての担保といった課題もポイント。そのようなファクターの検討要素は他には無いと思えばよろしいか。

伊地知構成員：現状の制度の中では、技術的な基準はかなり網羅をしている。しかし、事業者の財政基盤は見ていないのが実情。

吉田構成員：安心して国民に使ってもらうためには、事業の継続性も必要。ＥＵのＱＴＳＰはそのようなことまで含めて認定を受けているという認識。例えばヨーロッパのあるＱＴＳＰが潰れた際に、国で事業を継続するといったことが出来ている。

西山構成員：認定の単位は業務とするということに異論はない。しかし、サービスを特定する手段として、ポリシーや運用規程等を用いるというところに違和感がある。運用規程は業務を審査するときの規定文書ということで１つの対象とはなり得るが、利用者からすると、自分が今もらったタイムスタンプがどの運用規程に則って発行されているものかを本当に特定でき得るのかというと、できないと思う。

電子署名法では、鍵の認定とも考えられている。認定の対象となっている業務で使っている認証局の公開鍵証明書のハッシュ値を官報に公開している。指定調査機関のＪＩＰＤＥＣが特定認証業務の事業者のところに来て、鍵のハッシュ値を確認し、そのハッシュ値を主務三省の大臣に認定してもらうという構図。したがって、タイムスタンプが認定されたタイムスタンプかどうかということを、利用者が特定する手段としては、やはり鍵の認定というような概念に近いものを考えなければならない。

伊地知構成員：利用者がサービスを選ぶような局面においては、鍵単位で内容を確認する必要はない。ただ、実際にタイムスタンプを検証する局面においては、一つ一つのタイムスタンプが認定されたものなのかが非常に重要。公開鍵証明書をしっかりと特定できるというような仕組みをつくることが必要ということは強く同感。その必要性は、トラストリストなどの検討で明確にしていく必要がある。鍵のハッシュ値の確認はＪＩＰＤＥＣが立ち会うという説明があったが、タイムスタンプ局の場合、認証局に比べると鍵の生成の頻度が非常に多いため、立ち合いが難しい事情もある。バランスが重要だと認識。

吉田構成員：タイムスタンプはトラストアンカーの１つでもあり、異なる業務に亘って使っていくということが考えられる。当面は業務単位で認定していくというのはいいと思うが、将来的に、要するに、クロスインダストリーといった活用での認定制度を視野に入れていただきたい。

山内構成員：認定や認証に関する言葉遣いに十分留意すべきことに強く賛同。私は、当面は、認証と言わず、適合性評価という言葉を使いたい。そして、国の認定制度と、認定機関による適合性評価機関の認定とを区別したい。その上で、タイムスタンプの業務毎の適合性評価を、適合性評価機関が行うという形をとるのが良いと考える。認証局の世界では、事業を他社に譲渡することがある。そのため会社に着目するのではなくて、業務すなわちサービス自体の基準への適合性を評価することが大事。ＩＳＯ／ＩＥＣの世界では、ＩＳＯ／ＩＥＣ１７０６５という、製品、サービス、プロセス等に関する認証を行う適合性評価機関の要求事項がある。ただ、実際のサービスの適合性評価に際して、事業者の組織運営と分けて捉えるのは難しい。業務つまりサービス毎に適合性評価することになると、適合性評価機関は、サービスを提供する組織における運営がしっかりなされているかどうかも含めてサービスを認証し、さらに、その適合性評価機関を認定機関が認定するという形になっている。仮に、タイムスタンプの適合性評価においてＩＳＯの考え方を導入すると、ＩＳＯ／ＩＥＣ１７０６５が大きな役割を果たすと思う。タイムスタンプの場合、適合性評価機関は日本データ通信協会が担うと思うが、適合性評価機関自体の要求事項についても検討する必要がある。

伊地知構成員：国による指定になるのか、あるいは認定機関から適合性評価を受けて認定を受けるのかといったところは大きな論点。トラストサービスに関する認定のスキームに関してはＪＩＰＤＥＣにアドバイスをいただきたい。

山内構成員：事業者や組織の認証にするのか、それとも、サービスごとの適合性評価・認証にするのかは一番基本であり、重要な議論。

柿崎座長代理：認定の単位としてサービスというのは賛成。ただし、実質的にはタイムスタンプを付与するときに使われた署名鍵及びその対応する公開鍵証明書を特定する必要がある。タイムスタンプを検証するのは人間だけとは限らないため、機械が検証するということがこれから増えていくと考えられる。機械可読でかつ検証可能な状態にしておくことが重要。そのためには、公開鍵証明書等の特定を行っていく必要がある。

東條座長：既存の制度からのシームレスな移行という論点がある。これまで事業者単位で認定を行ってきたものをサービス単位に変更することは、認定事業者への影響という点では問題ないか。

事務局：資料作成の際に一部事業者にもヒアリングしたところ、サービス

単位のほうが分かりやすく、新たな事務的な負担はそれほど生じないという意見を伺った。

伊地知構成員：各認定事業者に対しては確認を取ったが、特段の問題点はないということで承っている。

東條座長：第１の論点ついては差し当たりよろしいか。

第２の論点、認定の対象とする時刻認証業務の技術方式については意見がないということで、続いて、第３の論点、申請者の条件について意見をお願いしたい。

上原構成員：もし、海外の事業者が同じ規格で認められるようなタイムスタンプを付与していたという場合、日本でそのタイムスタンプを受け入られるのかといった問題や、その事業者の活動を受け入れられるのかという問題は、別の協定に基づいた枠組みの中で行うという認識でよろしいか。

事務局：ＥＵとの相互認証というところになると思うが、例えば、ｅＩＤＡＳの規定によれば、基本的に他国との認証を求める場合、その国の法律の中身等が欧州委員会で法的に同等かを検証した上で、ＥＵの承認プロセスを経て、同等と見なされれば相互運用されていくということで、かなり長期的なスパンが必要だと認識。

伊地知構成員：国際相互承認については、当然、国同士の条約等の手続きが必要。ＩＳＯ１７０００や１７０６５などで規定をされている認定機関や適合性評価機関といった位置づけがあり、実際は、適合性評価機関同士が相互認証をするというケースや、認定機関同士が相互認証するというような手続が踏まれる場合もあると聞いている。国の制度が出来ることとは並行して、適合性評価を行う予定である我々がしっかりとその辺りも運用できるような状況にしていくことが重要だと認識している。

東條座長：本検討会では、法令改正までは視野に入れないという前提だが、ｅＩＤＡＳ規則の第 14 条に該当するようなものを日本でも策定するとすれば、どのような仕組みがあり得るか。

事務局：法制化は考えていない。電子署名は電子署名で、タイムスタンプはタイムスタンプでというように日 EU 間でいくつかの論点を用いて比較をしていく。Legally Equivalent というのは、必ずしも法律でないと同等とみなされないというわけではなさそうだという見解もある。欧州委員会の担当者や機関によって多少解釈も異なる。別途、協議していく必要があると思う。

山内構成員：「相互認証」という言葉を何人か使われたが、基本的には「国

際相互承認」という言葉遣いが適当。これは各国の間で適合性評価活動をした結果をお互いに受け入れるという意味での recognition を、Mutual Recognition あるいは Mutual Recognition Agreement、ＭＲＡと呼んでいるもの。もし言葉を使う場合には、相互承認あるいは国際相互承認やＭＲＡという言葉を使うのがいいと思う。

東條座長：要するに、本検討会の検討範囲は公的認定制度に限定する。また、３番目の論点は、海外の事業者の認定も受け付けるが、認定する際には、日本語で書類を全部作ることになるため、海外から認定を求める可能性は限定的であるということでよろしいか。

事務局：相互承認の話は本検討会のスコープ外だと認識。外国の事業者が日本のタイムスタンプ制度の認定を申請してくる際に認めるかどうかというのが申請者の条件で、日本の事業者と同様の基準で海外の事業者が申請をしてきた場合は、審査をした上で認定をしていくということ。あくまでも本検討会は認定の際の基準を議論いただくものだと認識。

小田嶋構成員：海外の事業者が申請できるということに関しては適当だと思っている。申請や調査の際には日本語での対応になると思う。その際の翻訳に関わるところといった手数料に関しては現地の業者が負うということに関しても記載した方がいいのではないか。

岩間構成員：申請できる者に海外の事業者も含めることには異論はない。ただ、過去、ＪＩＳを作ったときもそうだが、日本の認定制度ということで、時刻については、日本で唯一時刻を出しているＮＩＣＴの時刻を使うということをまず前提に作ってほしい。

伊地知構成員：ＩＳＯなどの基準や標準の中では、ＵＴＣ（ｋ）ということで、国際的な各機関（ｋ）のどこでもよいという規定になっている。日本ではこれをＪＩＳにするときに、ＵＴＣ（ｋ）と定義をしながらも、我が国においてはＵＴＣ（ＮＩＣＴ）を指すというような形で注釈がついている。この辺りについては、恐らくＴＡＡの扱いなどの論点で議論の対象になると思っている。

東條座長：ＥＵ以外の諸外国の仕組みとの整合性の観点からいうと、本日の３つの論点について特に問題はないと考えてよろしいか。

伊地知構成員：中国でも、デジタル署名方式が主流になっていると思われる。米国については、リンキングの方式を採用する事業者もあるが、マイクロソフトの例えばコードサイニング等には、デジタル署名の方式が使われている。恐らくデジタル署名方式が主流ということについては問題がない。

小木曽構成員：昨日資料が送られてきたばかりであり、会員にも展開できていないので、まず全ての論点について、新経済連盟としてはいいか悪いかということを含めて留保させていただく。それから、デジタル化していく中で、タイムスタンプの必要性というところがあるのは当然だが、それに対して、どういった打ち手を打っていくのかというところ。認定制度を作ること自体が目的ではなく、出口戦略を作っていく必要がある。一例として、トークンエコノミーの中で、ブロックチェーンを民法の第三者対抗要件として使えるようにする。また、民法の解釈の問題で、証書に関するものとして、押印、対面、書面原則の見直しに係る議論と関係してくると思うが、そのような内容も含めて議論すべき。利用者から見てどうかという視点が重要。会員へのアンケートも踏まえながら意見表明していきたい。

事務局：タイムスタンプ制度を作っただけでは使われない。利用者目線は重要である。現行でも幾つかの法令等、業界のガイドラインなどには、日本データ通信協会のタイムスタンプを使用して経理関係の書類を保存可能である等の規定もある。しっかり使っていただけるように我々も営業の努力をしていく。

吉田構成員：提案募集の結果も踏まえて、皆さんがこう使ったらいいのではないか、こういうところが必要ではないかというのを出していかなければならない。

東條座長：認定の対象に関する３つの論点について合意がされたということで取りまとめさせていただきたいと思う。

④　その他

事務局より次回の日程について説明があった。

（３）閉会

以上