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

令 和 ２ 年 １ ０ 月 ２ ０ 日

サイバーセキュリティ統括官室

「タイムスタンプ認定制度に関する検討会」論点全体像

タイムスタンプについて、国としての認定制度を創設するにあたって、今後検討・議論が必要であると考えられる論点（案）は以下のとおり。（赤字は本日の検討項目）

既に検討された項目
今回検討する項目
今後検討する予定の項目
検討継続中の項目

①認定の対象

- 認定の単位
  認定は、業務（サービス）単位とする
- 時刻配信・監査業務事業者（TAA）の扱い
  TSAが自らタイムスタンプの信頼性を確保する方式も認める
- 時刻認証業務の技術方式
  まずは、デジタル署名方式で制度を開始する
- 申請できる者の条件
  海外拠点で業務を行おうとする申請者も認める

②認定の基準

- 設備面の基準
  審査基準として、他の認証制度（コモンクライテリア等）も活用する
- 審査プロセス効率化
  他の認証制度を活用する

③認定の期間

- 認定の有効期間
  認定の有効期間は、2年とする

④調査機関の要件、調査・監査の在り方

- 調査を委託する機関に求められる要件
- 調査・監査の内容
  （諸外国や他のセキュリティ関連の制度も踏まえ、見直す必要があるか　等）
- 監査の在り方
  現行の制度と同様に内部監査も認め、年に1回実施することを求める

⑤認定業務の公表内容及び公表方法

- トラストリストへの記載事項等
  （諸外国との相互運用も踏まえながら、具体的な記載事項等を検討）

⑥その他

- 事業体として求められる要件
  認定・更新時の審査項目として、財務状況等を求める
- 廃止の場合の取扱い
  （諸外国や他のセキュリティ関連の制度も踏まえ、業務廃止の扱い等を検討）
- TSA公開鍵証明書を発行する認証事業者の基準
  （厳格に秘密鍵を管理している認証事業者、信頼のある監査機関からの監査を受けた認証事業者　等）
- 利用の拡大に向けた取組
  （関係省庁の制度や業界ガイドライン等でタイムスタンプを位置づけてもらうための働きかけ　等）
- 経過措置
  （国による認定制度へシームレスに移行する際に取るべき措置）

前回の論点について

○認定の対象

（1）TSAが自ら時刻の信頼性を確保する方式～時刻配信・監査業務事業者（TAA）の扱い～

【論点】

① 時刻の信頼性の担保

- トレーサビリティの起点となる時刻源は、日本標準時通報機関である「NICT」のUTC（NICT）とすべきか、各国の時刻標準機関 “k”によるUTC（k）でも可とするか。
- 発行されるタイムスタンプの時刻とトレーサビリティの起点となる時刻源の時刻差（時刻精度）の基準はどうあるべきか。
- タイムスタンプ発行前の時刻精度の確認（時刻が一定の基準内に収まっているかどうか）を要件として求めることが適切か。

② 時刻のトレーサビリティの担保

- TSAが自らトレーサビリティを立証するために、適切な機器のログを保管させることで十分か。
- 十分である場合、適切な「機器」、「ログ」とは何か。

【議論であがった主な意見】

- タイムスタンプ発行前の時刻精度の確認方法については、幅広く様々な方式を認めるのが適当。
- 時刻のトレーサビリティの担保にあたり、保管するログ等については証票類（例えば、電子署名法施行規則第12条第4号に規定する帳票類）も含めて考えるべき。

【方向性】

① 時刻の信頼性の担保

- トレーサビリティの起点となる時刻源は、日本標準時通報機関である「NICT」の**UTC（NICT）**とする。
- タイムスタンプトークンに記載される時刻について、**タイムスタンプ発行前に時刻精度の確認を行う**こととし、**トレーサビリティの起点となる時刻源との時刻差（時刻精度）の基準は、当該時刻源±1秒以内**とする。

② 時刻のトレーサビリティの担保

- 発行したタイムスタンプ時刻の時刻源に対するトレーサビリティをTSA自身が立証するために、**適切な機器における適切なログの保管**を行う。

前回の論点について

○認定の期間

(2)認定の有効期間

【論点】
- 認定の有効期間は、監査を含めた現行の制度を踏まえ、2年で十分か。
- 現行の制度及びEUの実態を鑑みて、認定の有効期間とTSA公開鍵証明書の鍵更新は切り離して考えることが適当か。

【議論であがった主な意見】
- 鍵更新や鍵の廃棄に関して監査等で十分にチェックされるのであれば、認定の有効期間は2年で問題ないのではないか。
- (参考)適切に鍵更新が行われていたかどうかを確認する手段として、タイムスタンプトークンのサンプリングチェックが考えられるのではないか。

【方向性】
- **認定の有効期間は2年**とする。

○調査機関の要件、調査・監査の在り方

(3)監査の在り方

【論点】
- 当該監査について、「現行の制度からのシームレスな移行」や「制度の普及・利用促進」の観点から現行の制度同様に内部監査も可能とすることが適切か、あるいは、EU等の「国際的な制度との整合性」の観点から、調査機関による監査を求めることが適切か。
  - ➢ 内部監査も可能とする場合:
    - ✓ 現行の制度と同様、年に1回規定することが適当か。
  - ➢ 調査機関による監査を求める場合:
    - ✓ 調査機関による監査を求める場合、調査機関に求める要件は何か。
    - ✓ 認定の有効期間内に少なくとも1回の監査を求めることで十分か。

【議論であがった主な意見】
- 内部監査の客観性、信頼性をいかに担保するかという点には配慮が必要。

【方向性】
- 現行の制度と同様、**内部監査も認める**が、必要に応じて外部監査も活用する。
- 監査は、**年に1回実施**することを規定する。

前回の論点について

○その他

（4）廃止の場合の取扱い

※継続検討

【論点】

- 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、廃止後に遅滞なく届出を求めることで十分か。
- TSA業務廃止による利用者への影響を考慮し、利用者へあらかじめ廃止の旨を周知することが必要か。
- その他の手続として、例えば総務省HPで公表といった国民への周知等、規定すべきことはあるか。

【議論であがった主な意見】

- 認定業務を公表することを考えると、廃止の届出は事後ではなく事前に求めるのが適当ではないか。
- 利用者の予見性の観点から、認定時に事業者に対して終了計画を策定させることが適切ではないか。
- 認定の段階で策定した終了計画が実際に廃止する際の事業者の過度な負担となり、また、認定時の手厚い終了計画を信用して契約した利用者に過剰な信頼を与える恐れがあるということにも考慮が必要。
- 継続性を保証するという点では、保険の活用についても検討の余地があるのではないか。

今回ご議論いただく論点について

○調査機関の要件、調査・監査の在り方

（1）調査・監査の内容

【現状・課題等】

～調査について～

- 日本データ通信協会の認定制度では、**「技術面」、「運用面」、「ファシリティ面」、「システムの安全性」、「情報開示にかかる事項」の5つの観点**で調査を実施。
- 認定制度の運用が始まってからこれまで、必要に応じて審査基準（調査内容）の改訂を実施。
- なお、これまでの検討会では、**新たな観点として「事業体として求められる要件」**が方向性として示され、既存の観点においても、「TSA自ら時刻の信頼性を確保する方式」や「時刻認証業務の技術方式」、「HSMの要件」等について、それぞれの方向性が示されている。

～監査について～

- 日本データ通信協会の認定制度では、監査にて**審査基準の全項目**を実施することを規定。
- （参考）なお、頻度は年に1回以上で、内部監査も認めている。
- EUでは、適合性評価機関によるサーベイランス監査を実施することを規定しており、24か月に1回、**フル監査の50%程度の内容**※1を実施。

※1　野村総合研究所によるTUVへのヒアリング結果より（総務省委託事業）

【論点】

- これまで検討会で示された方向性や議論等を踏まえ、調査の観点については、現行の制度における5つの観点に加え、「事業体の要件」を追加することで十分か。
- 監査の内容について、現行の制度では全項目を確認しているが、EUの実態も踏まえて内容を省略する余地はあるか。
- 監査の内容（新規・更新認定における全項目の確認）を省略する余地がある場合、どのような観点で省略する項目を検討することが適切か。

今回ご議論いただく論点について

○その他

(2)TSA公開鍵証明書を発行する認証事業者の基準

【現状・課題等】

※1　実態としてWeb Trust認証に限定されている

- **電子署名法の認定認証事業者と同等の認証局(CA:Certification Authority)**、または、**信頼のある監査機関の監査※1に適合したCA**等であることを審査基準に規定。
- 上記の基準が不明確で、**TSAがCAを選定・判断することが困難**であることが課題。
- なお、上記の規定で担保しているのは、当該CAが一定の水準を満たす事業者であるいうことにとどまり、実際に当該CAがTSA公開鍵証明書の発行業務を行う際に、例えば適切な体制・設備で行っているかどうかは担保できていないことも課題。(CAは現行制度における認定の対象外であるため、TSA公開鍵証明書を発行する際の具体的な要件(体制・設備等)をCAに対して求めることは困難)
- 他方、万が一TSA公開鍵証明書発行業務に不備等が発生した場合は、当該CAの信頼に関わる問題となり、認定・認証を受けた業務にも支障をきたし得る。
- EUでは、**TSA公開鍵証明書は適格認証事業者によって発行**されるべきであることをETSIで規定。

【論点】

- TSAがCAを選定・判断できるよう、TSA公開鍵証明書を発行するCAの基準を明確にすることが適切か。
- 明確にすることが適切である場合、その基準は電子署名法の認定認証事業者、または、Web Trust認証を受けた事業者であることを求めることが適切か。
- 電子署名法の認定やWeb Trust認証以外に、他の認証制度や認定制度の活用の余地がある場合、どのような制度の活用が考え得るか。

これまでご議論いただいた論点について

○調査機関の要件、調査・監査の在り方

(3)調査を委託する機関に求められる要件

※一部再掲

【論点】

- 国の認定制度においても、第三者機関に調査を行わせることができるようにすることが適当か。
- 第三者機関の要件については、電子署名法の規定を踏まえて、検討することが適当か。

【議論であがった主な意見】

- 電子署名法の指定のような方式をとるとしても、EUの制度といった国際的な制度との整合性は重要ではないか。

【ご意見を踏まえた事務局の見解】

- 行政事務の簡素化や民間能力の活用の観点から、**民間の第三者機関に調査を行わせることができるようにすることが適当**ではないか。
- 今回は個別のトラストサービス(タイムスタンプ)に関する検討であることから、調査を委託する機関の要件は、基本的には**電子署名法の指定調査機関の指定の基準をもとに検討することが適当**ではないか。
- 今後トラストサービスの包括的な制度検討を行う場合には、必要に応じて国際標準であるISO/IEC17065やEUの標準であるEN 319 403を活用した要件を参考にすることは有用ではないか。

【参考】

電子署名法

第二十条　主務大臣は、指定の申請が次の各号のいずれにも適合していると認めるときでなければ、その指定をしてはならない。

一　調査の業務を適確かつ円滑に実施するに足りる経理的基礎及び技術的能力を有すること。

二　法人にあっては、その役員又は法人の種類に応じて主務省令で定める構成員の構成が調査の公正な実施に支障を及ぼすおそれがないものであること。

三　調査の業務以外の業務を行っている場合には、その業務を行うことによって調査が不公正になるおそれがないものであること。

四　その指定をすることによって申請に係る調査の適確かつ円滑な実施を阻害することとならないこと。

これまでご議論いただいた論点について

○認定業務の公表内容及び公表方法

(4)トラストリストへの記載事項等

【論点】 ※一部再掲

- 認定を受けたタイムスタンプかどうかをユーザー側で識別することができるための情報として、どのようなものが考え得るか。
- それ以外に公開すべき情報として、どのようなものが考え得るか。
- 以上の情報をトラストリスト(仮)として、総務省HPへ公開することで十分か。

【議論であがった主な意見】

- 誰が何のためにタイムスタンプを検証するのかという観点で、トラストリストに掲載する項目を検討することが重要。
- 公開すべき内容としては、法人番号、業務の名称・業務を行う者の名称(英文併記)、TSA公開鍵証明書のハッシュ値、公開鍵証明書、認証局の証明書等があげられるのではないか。
- EUのトラストリストのような仕組みで、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が望ましい。
- ヒューマンリーダブルな形式がサービス選択を行う際の手がかりとなる一方で、マシンリーダブルな形式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。

【ご意見を踏まえた事務局の見解】

- 公開する必要のある情報として、**当該業務を特定可能な情報**(業務の名称、TSA公開鍵証明書及びその公開鍵のハッシュ値等)及び**当該業務を実施する者を特定可能な情報**(法人番号、業務を行う者の名称(英文併記)等)が考えられるのではないか。
- タイムスタンプの自動的な検証の観点から、現行のヒューマンリーダブルな形式のみならず、**マシンリーダブルな形式でも公表することが有用**ではないか。
- タイムスタンプの長期的な検証の観点から、**過去の履歴情報もあわせて公開することが有用**ではないか。
- 他方、**マシンリーダブルな形式での公開及び履歴情報を含めた公開については、**トラストサービス横断的な要素も考えられることから、具体的なデータ形式や構造等を含め、**将来的には別途検討が必要**であると認識。

これまでご議論いただいた論点について

○その他

(5)廃止の場合の取扱い

※一部再掲

【論点】

- 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、廃止後に遅滞なく届出を求めることで十分か。
- TSA業務廃止による利用者への影響を考慮し、利用者へあらかじめ廃止の旨を周知することが必要か。
- その他の手続として、例えば総務省HPで公表といった国民への周知等、規定すべきことはあるか。

【議論であがった主な意見】

- 認定業務を公表することを考えると、廃止の届出は事後ではなく事前に求めるのが適当ではないか。
- 利用者の予見性の観点から、認定時に事業者に対して終了計画を策定させることが適切ではないか。
- 認定の段階で策定した終了計画が実際に廃止する際の事業者の過度な負担となり、また、認定時の手厚い終了計画を信用して契約した利用者に過剰な信頼を与える恐れがあるということにも考慮が必要。
- 継続性を保証するという点では、保険の活用についても検討の余地があるのではないか。

【ご意見を踏まえた事務局の見解】

- 認定を受けた業務の適切なタイミングでの公表を考慮し、TSAから主務省への**廃止の届出は事前に求めることが適切**ではないか。
- 認定を受けた業務について、認定時に詳細な終了計画(業務の引継ぎ先に関する規定やエビデンスの移管に関する規定等)を求めることは、利用者に一定の安心感を与える一方、不測の事態等による廃止の際に、策定した終了計画によって速やかな撤退ができず、当該TSAに過度な負担がかかる可能性があることや、利用者に過剰な信頼を与える懸念があることから、**退出規制については慎重な検討が必要**ではないか。
- 上記を踏まえ、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**ではないか。
- なお、**終了計画として規定すべき項目**については別途検討が必要。
  (例:利用者への事前通知に必要な期間、タイムスタンプの継続的な検証に係る項目、鍵の安全な廃棄及びその過程の記録・報告に関する事項 等)

（参考）検討に当たっての主な観点

１．既存の制度からのシームレスな移行

- 既存の日本データ通信協会の認定制度における認定事業者への影響
- 現在の日本データ通信協会のタイムスタンプ認定制度を引用している関係省庁の法令等や業界ガイドラインへの影響　等

２．国際的な制度との整合性

- EU等の諸外国の制度との整合性
- ISO等国際標準との整合性　等

３．制度の普及・利用促進

- 監査（調査）やサービス提供のコスト面への影響
- サービス利用者の立場から見ても、その信頼性担保の仕組みがわかりやすい制度設計（例：トラストリスト）が必要　等