資料６－１

タイムスタンプ認定制度に関する検討会（第６回）
事務局資料

令 和 ２ 年 ９ 月 ２ ３ 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
  （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）

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
  （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）

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

○認定業務の公表内容及び公表方法

(1)トラストリストへの記載事項等

※継続検討

【論点】

① 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。

② 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。

③ 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。

○その他

(2)事業体として求められる要件

【論点】

① 業務(サービス)を維持及び適格に遂行可能かどうかの基準として、財務状況等の要件を求める必要があるか。

② 財務状況等を要件として求める場合、審査項目として規定することが適切か、欠格条項として規定することが適切か。

【議論であがった主な意見】

- 既存の制度を踏まえると、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**ではないか。

【方向性】

事業体として求められる要件として、現状規定している技術的能力に加えて、**財務状況等も審査項目として規定**する。

今回ご議論いただく論点について

○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～

① 時刻の信頼性の担保

【現状・課題等】

- 日本データ通信協会の認定制度では、**TAA方式に限定**している。
- EUは、**少なくとも1つ以上の各国の時刻標準機関“k”によるUTC（k）にトレーサブルであることを規定**している。
- 日本データ通信協会の認定制度もEUも**一定の時刻精度（時刻源±1秒）を逸脱するタイムスタンプを発行してはならないことを規定**している。なお、時刻精度の確認は特定の手段に限定していない。
- 中国は認定制度は存在しないが、TSAが参照している中国国家（推奨）規準では、**UTC（NTSC※1）への同期**を求めている。

※1　中国国家時刻標準機構である「国家授時センター」

【論点】

- 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

【現状・課題等】

- 日本データ通信協会の認定制度では、時刻のトレーサビリティに関し、**TAAによる監査記録を保存することを規定**している。
- EUでは、**タイムスタンプサーバーに保存されるログを適切な期間※2保存することを規定**している。
- 中国では、中国国家（推奨）規準において、内部監査用に、時刻同期等の各種ログの記録について基準を示している。

※2　明確な期間の規定はないが、多くの場合がTSA公開鍵証明書の有効期限（通常1～3年）が切れてから10年としている

【論点】

- 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。

今回ご議論いただく論点について

○認定の期間

(2)認定の有効期間

【現状・課題等】

※一部再掲

- **日本データ通信協会の認定制度の認定の有効期間は2年と規定**している。
- 年に1回以上の自主監査(内部監査(部署外)でも可)を義務付けているところ、有効期間が2年であっても、これまでタイムスタンプの信頼性に係る問題は発生していない。
- EUにおいても、認定の**有効期間は2年**であるが、認定の有効期間内(24か月)に1回、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で適切な認定の状態を維持している。
- なお、**電子署名法における認定の有効期間**については、立法当時、諸外国の認定制度を踏まえて、**1年と規定**している。

【議論であがった主な意見】

- EUとの整合性を考えると、**2年が適切**ではないか。
- 日本では鍵更新が毎年あることを踏まえると、監査のやり方等の制度設計について工夫が必要ではないか。
- **鍵更新との関係を整理せずに2年という結論は出せない**のではないか。

～TSA公開鍵証明書の鍵更新について～

- 日本データ通信協会の認定制度は、認定の有効期間が2年であるが、毎年行っているTSA公開鍵証明書の鍵更新との関連性はない。(なお、鍵更新が適切に行われたかどうかは、認定更新の調査で確認している。)
- EUでは、認定の有効期間は2年であり、TSA公開鍵証明書の鍵更新(通常1～3年)との関連性はない。(なお、鍵更新が適切に行われたかどうかは、そのエビデンスをサーベイランス監査で確認。)

【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。

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

(3)監査の在り方

【現状・課題等】

- 日本データ通信協会の認定制度では、TSAに対して、**年に1回**、新規及び更新認定と同じ調査内容の**自主監査を実施することを規定**している。
  (**内部監査(部署外)又は外部の機関による監査も可**)
- 現行の制度においては、年に1回の自主監査の仕組みで、これまで認定の適否に係る問題やタイムスタンプの信頼性に係る問題は生じていない。
- EUでは、TSAの認定の状態を維持するために、**認定の有効期間内(24か月)に1回**、新規及び更新認定の約50%の内容の**サーベイランス監査を適合性評価機関によって実施することを規定**している。
- 中国には認定制度は存在せず、中国国家(推奨)規準においても、監査に関する規定はない。
  ただし、NTSCと唯一正式に業務提携をしているTSAである北京聯合信任技術サービス有限公司(UTSA)は、毎年第三四半期に、中国科学院(NTSCが所属する国家部門)の年度監査を受ける必要がある。

【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。

今回ご議論いただく論点について

○その他

（4）廃止の場合の取扱い

【現状・課題等】

- 日本データ通信協会の認定制度では、運用規定にて、TSAが業務を廃止した際の**事後的な届出の提出**を規定。また、審査基準に**利用者に対する事前通知を規定**している。
- 現行の制度において、TSA業務廃止の実績はあるが、**実際の廃止時及び廃止後に特段の問題は生じていない**。
- 電子署名法では、**あらかじめ業務廃止の旨を主務大臣に届け出なければならない**ことを規定している。また、**主務大臣は、その旨を公示しなければならない**ことを規定している。
- 国内の認定業務として、
  - 放送法では、業務廃止の際は、その旨を**総務大臣に届け出なければならない**ことを規定している。
  - 電気通信事業法では、電気通信業務の全部又は一部を廃止しようとするときは**あらかじめ利用者に必要な事項を周知**させることを規定している。（利用者への利益に及ぼす影響が大きいものは、あらかじめ総務大臣への届出を規定）
- EUでは、**利用者、監督機関、依拠当事者（署名検証者）等への廃止の旨の事前連絡・通知**、**業務の運用にかかるエビデンスに関する情報**や**タイムスタンプの検証に必要な情報等の保持**について規定。
- 中国は、認定制度がなく、国家（推奨）規準でも業務の廃止に関する規定はない。

【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。

【参考】

電子署名法

第十条　認定認証事業者は、その認定に係る業務を廃止しようとするときは、主務省令で定めるところにより、あらかじめ、その旨を主務大臣に届け出なければならない。

２　主務大臣は、前項の規定による届出があったときは、その旨を公示しなければならない。

（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