資料３－１

タイムスタンプ認定制度に関する検討会（第3回）
事務局資料

令 和 ２ 年 ５ 月 ２ ９ 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**）

※ タイムスタンプ認定制度に関する検討会（第1回）資料1－2 論点案 再掲

■ 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

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**
  （現在、認定の対象であるTAAの扱いについて 等）
- **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**
  （HSMのセキュリティレベルの要求要件について見直す必要があるか）
- **審査プロセス効率化**
  （運用基準の審査に当たり、ISO認証等の取得をもって代替できるか）

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（監査）機関の要件、調査（監査）のあり方

- 調査（監査）を委託する機関に求められる要件
- 調査（監査）の頻度、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）

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
  （諸外国との相互運用も踏まえながら、具体的な記載事項を検討）

⑥その他

- 廃業の場合（TSA又は認証局）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、廃業時の扱い等を検討）
- 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）認定の単位

- 認定された業務を利用者が明確に特定・把握できることが必要
- 電子署名法においても、認定の単位は業務
- EUにおいても、認定の単位は業務

【方向性】

- 認定は業務（**サービス）単位**とする。

（補足）

TSA公開鍵証明書の扱いについてトラストリストの記載事項の論点で検討が必要。

（2）認定の対象とする時刻認証業務の技術方式

- 日本においては、デジタル署名方式が主流（6社中5社）※
- EU・中国・米国においても、デジタル署名方式が主流

※ 残り1社はリンキング方式で2020年8月に業務廃止予定

【方向性】

- 審査の効率性の観点から、まずは**デジタル署名方式**で制度を開始する。

（3）申請者の条件

- 電子署名法では、外国の事務所により特定認証業務を行う者の申請を認めている。

【方向性】

- 国内に限定せず、**外国の事業者の申請も可能なものとする**。

（補足）

- 海外の事業者であっても、日本の時刻を使うということを前提にすべきではないか。
- 海外の事業者であっても、国内の事業者と同様の審査を行うことを前提とする。

今回ご議論いただく論点について

○認定の対象

（1）時刻配信・監査業務事業者（TAA）の扱い

【日本データ通信協会の認定制度】
- 日本データ通信協会の認定制度では、タイムスタンプの信頼性を担保する方式について、**TAA方式に限定**。

【現状・課題等】
- 例えば、**TAAが停止した場合**、当該TAAから時刻の配信を受けている**TSAのタイムスタンプサービスがすべて停止**してしまうことや、TSAがTAAを利用するコストが**タイムスタンプ利用料へ影響**してしまっていること等が課題。
- 他方、**EUや中国ではTAA方式以外の方式が主流**であり、**TSAが自らタイムスタンプの信頼性を確保する方式**であっても、**十分なタイムスタンプの信頼性を備えている**。

【方向性】
- タイムスタンプの国としての認定制度の検討に当たっては、タイムスタンプの信頼性確保に関して、TAA方式に限定せず、**TSAが自らタイムスタンプの信頼性を立証する方式も認めることが適当**ではないか。

今回ご議論いただく論点について

○認定の基準

(2)設備面の基準

【日本データ通信協会の認定制度】

- タイムスタンプトークンの生成に用いる秘密鍵を格納するHSMについて、FIPS140-2のレベル3認証相当以上の製品に限定。

【現状・課題等】

- 当該基準を満たしたHSMは世界的にも限定的で継続的な調達の不安や、障害発生時の予備機の確保などのTSAのコスト負担等が課題。
- 他方、現状の認定制度におけるHSMに対するセキュリティ要件(秘密鍵の保護)は適切。
- EUにおいては、トラストサービスに用いられるHSMに必要な要件を満たしたコモンクライテリアに基づく認証を受けたHSMも認めており、より裾野が広い。

【方向性】

- タイムスタンプサービスに求められるHSMの要件を満たした他の認証制度(例えば、コモンクライテリア)を活用することで、調達先の裾野を広げていくことが適当ではないか。

(3)審査プロセス効率化

【検討の視点】

- 既存の認証制度(ISMS認証、プライバシーマーク制度　等)の活用の余地。
- 電子署名法の認定制度において、提出を求めている書類の中で重複する資料の活用の余地。

【方向性】

- 他の認証や既存の制度等を活用し、具体的な審査項目を省略することで、審査を行う側と受ける側の双方の効率化を図ることが適当ではないか。

（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