資料５－１

タイムスタンプ認定制度に関する検討会（第５回）
事務局資料

令　和　２　年　８　月　７　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）
- 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
  （既存の制度（電子署名法、情報銀行 等）を踏まえながら、要件を検討）
- 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）時刻配信・監査業務事業者（TAA）の扱い

※継続検討

【論点】

① 時刻の信頼性の担保
- TAA以外の**時刻源は、どのような選択肢が考えられるか**。
- タイムスタンプ発行前の時刻精度の確認として、**時刻チェック用の時刻源が別に必要か**。
  また、必要であれば、**どのような時刻源の選択肢が考えられるか**。

② 時刻のトレーサビリティの担保
- トレーサビリティを担保するために、どのような情報をどれくらいのサイクル・期間保存する必要があるか。

【議論であがった主な意見】
- 時刻源は、日本標準時に準拠すべきであり、UTC(NICT)を採用することが適切ではないか。
- 時刻精度の確認のため、経路等異なる時刻源を使ったチェック機構が必要ではないか。
- トレーサビリティとしては、各機器における上位のNTPサーバとの時刻同期ログを保存し、開示できるようにしておく必要があるのではないか。

○認定の期間

（2）認定の有効期間

※継続検討

【論点】

① **認定の有効期間は**、現行の制度を踏まえ、**2年で十分か**。

② 電子署名法における認定の有効期間が1年であることを踏まえ、タイムスタンプの**認定の有効期間を1年とする事情はあるか**。

【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。

○調査機関の要件、調査・監査の在り方

（3）調査機関の要件

※継続検討

【論点】

① 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**。

② **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。

今回ご議論いただく論点について

○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

【現状・課題等】

- 日本データ通信協会の認定制度では、**①氏名又は名称及び法人にあっては、その代表者 ②認定に係る業務の種類 ③住所 ④認定日及びその更新日並びにその有効期間を協会のウェブページに公開**。
- **認定を受けたタイムスタンプか否か識別することが困難**であることが主な課題。
- 電子署名法においては、**①特定認証業務の名称、②当該業務を行う者の名称及び③住所、④認定の年月日及び⑤その効力を失う年月日、⑥発行者署名検証符号に係る電子証明書の値をハッシュ関数で変換した値を官報に掲載**。(電子署名法第4条第3項、施行規則第15条)
- EUにおいては、トラストリスト(機械可読形式)として、**当該サービスの情報やステータス等を公開**。

【論点】

- 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。(例:業務(サービス)名、TSAの公開鍵証明書 等)
- 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。(例:法人番号、事業者名 等)
- 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。

【参考】

(電子署名法逐条解説抜粋)

①認定を受けた認証事業者の氏名・名称、住所、代表者(法人の場合)、②認定を受けた特定認証業務(サービス名称等)、③認定を受けた日などを官報に公示することを予定している。

今回ご議論いただく論点について

○その他

(2)事業体として求められる要件

【現状】

- 日本データ通信協会の認定制度では、TSAに対しては**欠格条項を規定**し、TAAに対しては**欠格条項に加えて経営情報開示の基準を規定**。
- 電子署名法の認定制度では、認定認証事業者に対して**欠格条項を規定**。
- 他方、放送法や電気通信事業法では、**認定の基準として経理的基礎**及び技術的能力**を規定**。
- その他の認定制度(民間)として、
  - 情報銀行認定制度においては、**財務状況**等を規定。
  - ASP・SaaS安全・信頼性に係る情報開示認定制度※1においては、**財務状況**や**コンプライアンス**等に関して規定。
- EU(eIDAS規則)においては、**財政基盤**等を規定。

※1 クラウドサービスのサービスのうち安全・信頼性に係る情報を適切に開示しているものに関する認定制度

【論点】 ※現状規定している「欠格条項」については、引き続き規定することを前提とする

- 業務(サービス)を維持及び的確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。(技術的能力については、現状も規定しており、引き続き規定することを前提とする)
- 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。

【参考】

電子署名法

第五条 次の各号のいずれかに該当する者は、前条第一項の認定を受けることができない。

一 禁錮以上の刑(これに相当する外国の法令による刑を含む。)に処せられ、又はこの法律の規定により刑に処せられ、その執行を終わり、又は執行を受けることがなくなった日から二年を経過しない者

二 第十四条第一項又は第十六条第一項の規定により認定を取り消され、その取消しの日から二年を経過しない者

三 法人であって、その業務を行う役員のうちに前二号のいずれかに該当する者があるもの

（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