資料４－１

タイムスタンプ認定制度に関する検討会（第４回）
事務局資料

令　和　２　年　７　月　１　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
新たに追加した項目

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
  （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

- 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

- タイムスタンプの信頼性確保のためには、①時刻の正確性、②時刻のトレーサビリティの担保が重要
- TAA方式によらずとも、TSA自らが①及び②を立証し、担保することが可能
- EUや中国においても、「TSAが自ら立証する方式」が主流であり、十分なタイムスタンプの信頼性を備える

【方向性】

- タイムスタンプの信頼性確保に関して、**「TSAが自ら時刻の信頼性を担保する方式」も認める**。

（補足）
我が国で採用する具体的な方法については、要検討。

○認定の基準

（2）設備面の基準

- 現在の日本データ通信協会の基準（FIPS140-2レベル3認証相当以上）を満たした調達可能なHSMは、限定的かつ高コスト
- 現状のHSMに求められているセキュリティレベルは必要最低限
- EUでは、トラストサービス用の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製品も認めており、調達の裾野が広い

【方向性】

- 裾野を広げるために、HSMの基準として、現行のFIPSの基準に加え、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（コモンクライテリア等）も活用する**。

（補足）
我が国で選択するタイムスタンプに用いるHSMについてのコモンクライテリアの要件は要検討。

（3）審査プロセス効率化

- 既存の認証制度（ISMS認証、プライバシーマーク制度　等）の活用への期待。
- 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への期待。

【方向性】

- 審査プロセス効率化の観点から、**他の認証**（ISMS等）や**既存の制度**（電子署名法等）**も活用する**。

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

【前回示した方向性】

- タイムスタンプの信頼性確保に関して、**「TSAが自ら時刻の信頼性を確保する方式」も認める**。

【論点】

タイムスタンプの信頼性を確保するために重要な**①時刻の信頼性の担保**、**②時刻のトレーサビリティの担保**について、可用性やコスト面を考慮しつつ、以下を検討する必要があるのではないか。

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**。

（参考）日本データ通信協会の認定制度では、UTC（NICT）との同期精度を±1秒以内に規定

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。

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】

- **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**。
- 年に1回以上の部署外からの監査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**。
- 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。

【論点】

- **認定の有効期間は**、現行の制度を踏まえ、**2年で十分か**。
- 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**。

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)調査機関の要件

【現状】

- **日本データ通信協会の認定制度**においては、**認定主体と調査主体がともに日本データ通信協会**。
  - 制度運用規定のみで、調査機関に関する要件は定められていない
- **電子署名法**の認定制度においては、**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規定**。
- EU(eIDAS規則)においては、認定主体は各国(EU加盟国)が指定した監督機関で、調査(適合性評価)主体は各国指定の認定機関が認定した適合性評価機関。
  - 適合性評価機関に求められる要件としては、財務上の安定性及び運営に必要な経営資源をもつこと、適合性評価以外の活動が適合性評価の公平性に影響しないこと　等があげられる

【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**。

【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**。

（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