第4回 タイムスタンプ認定制度に関する検討会

資料４－２

各論点について

2020年7月1日

タイムビジネス認定センター長
伊地知　理

一般財団法人
日本データ通信協会

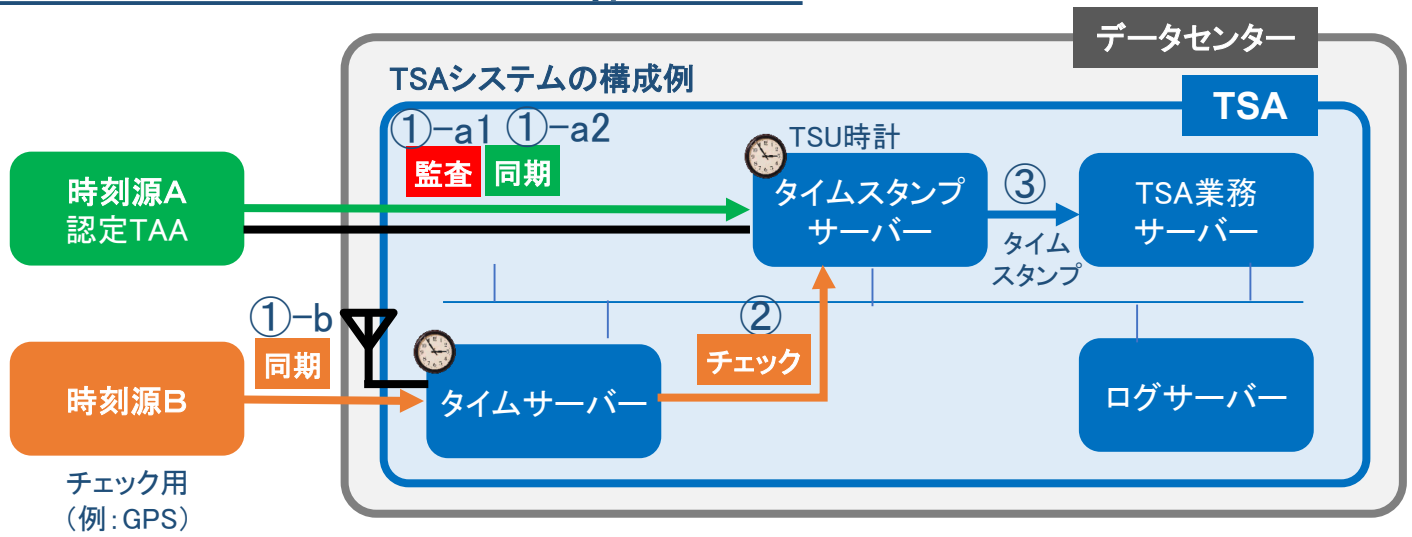
1. 認定の対象　②’タイムスタンプ時刻の信頼性

TAAを使用する方式のTSAシステム構成例

①-a1：定期的に認定TAAがTSU時計を監査し、誤差が閾値を越えている場合、TSAに通知する。タイムスタンプ発行機能を停止することもできる。
①-a2：定期的に、TSU時計の時刻を時刻源A（認定TAA）に同期させる。
①-b：既定の頻度でタイムサーバーは、時刻源Bに同期する。

②：タイムスタンプサーバーは、適宜、タイムサーバーを参照し、TSU時計と比較する。

③：②で正常の場合、リクエストを受けてタイムスタンプを発行する。なお、比較結果に異常があればタイムスタンプ発行を停止する。



- TSA自ら時刻の信頼性を確保する方式の論点
  - ①時刻の信頼性をどのように担保するか
    - A） TAAに替わる時刻源として、何が対象として考えられるか、1つでいいのか、複数必要か
    - B） タイムスタンプ発行前の時刻精度チェック用の時刻源は必要か、必要な場合は何が選択肢として考えられるか
  - ②時刻のトレーサビリティをどのように担保するか
    - 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

1. 認定の対象　②’タイムスタンプ時刻の信頼性

TSA自ら時刻の信頼性を確保する方式の時刻源

①TAAに替わる時刻源及びチェック用の時刻源として、何が対象として考えられるか？

分類	時刻源	同期するUTC	特徴	メリット	デメリット
NICTが提供する時刻源	時刻情報提供サービス	UTC（NICT）	個別契約に基づきNICT内に通信機器を設置し専用線等で接続する。	時刻トレーサビリティの確保が確実。安定した時刻情報の提供が受けられる。	NICT設置分も含め専用線等の回線費用がかかる。
	光テレホンJJY	UTC（NICT）	ひかり電話を用い1時間に1回程度同期する。		回線費用がかかる。
	長波JJY	UTC（NICT）	一般の電波時計で用いられる時刻源。	通信費が発生しない。	時刻トレーサビリティの確保は、同期した側のログ等に依存する。**妨害電波等の攻撃のリスク**がある。
衛星を用いた時刻源	GPS	UTC（USNO）	GPSは歴史が古く対応したタイムサーバー製品も多い。みちびき、Galileoに対応した製品はGPSに比べると少ない。また「みちびき」だけ受信する製品もない。	通信費が発生しない。	時刻トレーサビリティの確保は、同期した側のログ等に依存する。**妨害電波等の攻撃のリスク**がある。 アンテナ設置工事等が発生する。
	みちびき	UTC（NICT）			
	Galileo※1	複数UTC（k）			
公開NTPサーバー	NICT	UTC（NICT）	NTPプロトコルを用いて時刻サーバーを提供するもの。運営者が何らかの時刻源に同期する仕組みを構築している。	一般のサーバー等がNTPプロトコルに対応しており、専用のタイムサーバーが必須ではなくなる。	時刻トレーサビリティの確保は、同期した側のログ等に依存する。 **なりすまし等のリスク**がある。
	データセンター各社	運営者に依存			
その他の時刻源	NHK FM時報	UTC（NICT）	NHK FMラジオの時報に合せるもの。	GPS等よりも受信できる環境を得やすい。	正時のタイミングに合わせるのみで、日付も時刻も得られない。

※1　Galileoの時刻系（GST）は、フランス、ドイツ、イタリア、スペイン、スウェーデンで実施されているUTCの全国リアルタイム概算と継続的に比較することによってUTCと50ナノ秒以内で同期することを目標としている。

1. 認定の対象　②’タイムスタンプ時刻の信頼性

TSA自ら時刻の信頼性を確保する方式の検討の視点

② 時刻の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

- （参考）現行の日本データ通信協会（TAA方式）では、TAAにおいて、時刻差証明書※1及びその発行記録の保存を求めている
  - TAAは、タイムスタンプの有効期間等を考慮し、運用規程に10年以上の保存を定めている。
- （参考）EUでは、TSAにおいて、TSU時計とUTCとの同期に関するすべての事象に関する記録を保存することを求めている

※1　TAAがTSAに対して時刻監査を行い、測定した結果を証明するために発行するもの。JIS規格では24時間以内の間隔で当該証明書を発行することが望ましいとしており、実際には、TAAは数時間ごとに発行している。

③認定の期間（認定の有効期間）

認定の有効期間の選択肢

現行制度が2年としているところ、電子署名法の例にならい1年とするか、または、事業者負担の軽減が期待される3年に延長する可能性について検討が必要

期間の選択肢	メリット	採用した場合の問題点等
1年 （電子署名法）	・更新審査の間隔が短くなることで、万が一、不適合状態が生じていても、早い段階で検知できる。	・更新審査に係る事業者及び調査機関の負担が大きくなる。
2年 （現行制度、情報銀行、EU）	・現行制度は2年で安定的に運用されており、円滑な制度の移行が可能。 ・デジュールスタンダード※1策定で先行しているEUも2年であり国際相互承認における親和性が高い。	・万が一、不適合状態が生じていた場合の検知が、「1年」の場合よりも遅くなる。
3年 （ISMS）	・更新審査の間隔が長くなることで、更新審査に係る事業者の負担が軽減される。	・EUが2年であり国際相互承認の交渉で受け容れられないリスクがある。 ・万が一、不適合状態が生じていた場合の検知が、「1年」や「2年」の場合よりも遅くなる。

※1 標準化団体によって定められた標準規格のこと

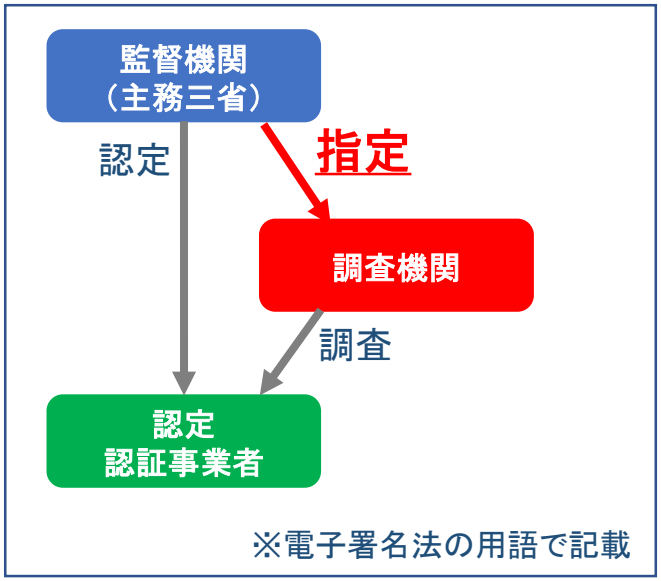
③認定の期間（認定の有効期間）

認定の有効期間の現状

- 現行の制度において有効期間2年で運用を行い、年に1回以上の自主監査を行っており、タイムスタンプの信頼性に係る問題等は生じていない。
  - 自主監査は、部署外（社外またはチェック機能の働く社内の別組織）の監査人が、審査基準に基づき全項目の監査を行うこと、及び、監査結果を日本データ通信協会に開示することを求めている。
  - 自主監査で、不適合が指摘されていれば、日本データ通信協会による調査を行い改善要請を行う場合もある。
- EUも24ケ月に1回以上、適合性評価を受ける必要があり、加えて、年に1回以上のサーベイランス監査の実施を推奨している。

④調査（監査）機関の要件

電子署名法の枠組み



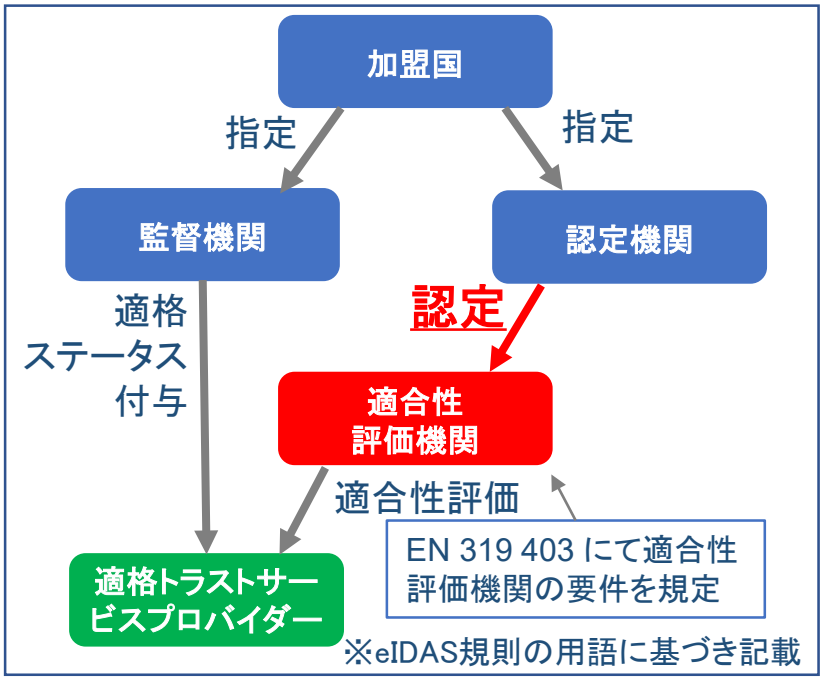
調査機関の指定の基準(電子署名法第20条)

- 経理的基礎及び技術的能力を有すること
- 役員の構成が調査の公正な実施に支障を及ぼさないこと
- 調査の業務以外の業務により調査が不公正にならないこと
- 指定により調査の適確かつ円滑な実施を阻害しないこと

- 指定の有効期間：5年（法第22条第1項、施行令第2条）
- 秘密保持に関する事項（法第23条）
  - ➢ 調査の業務に関して知り得た秘密を漏らしてはならない
- 調査業務に関する事項（法第25条）
  - ➢ 調査の業務に関する規定を定め、主務大臣の認可を受けなければならない
    - ✓ 調査の業務関する秘密の保持に関する事項、調査の業務に関する帳簿及び書類の管理に関する事項 等
      （指定調査機関等に関する省令第8条第6号、7号）

④調査（監査）機関の要件

eIDAS規則の枠組み



- EUにおける認定の仕組み（EN 319 403, ISO/IEC 17065）
  - 財務上の安定性及びその運営に必要な経営資源をもたなければならない
  - その運営から生じる債務を担保できる適切な備え（例えば，保険又は準備金）をもたなければならない。
  - 公平性に対するトップマネジメントのコミットメントがなければならない。
  - 適法性評価以外の活動が適合性評価の公平性を損なわないこと　他

END

各論点について

タイムビジネス認定センター