第7回 タイムスタンプ認定制度に関する検討会

資料７－２

各論点について

2020年10月20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. 調査・監査※1の内容

【調査の内容】

現状（タイムビジネス信頼・安心認定制度）の調査内容

- 5つの観点で審査基準を策定している
  - 技術基準
    - タイムスタンプの時刻精度に係る項目、タイムスタンプトークンの形式や暗号技術に係る項目、TSA公開鍵証明書に係る項目、他を規定
  - 運用基準
    - 専門性の優れた要員を配置し独立性が確保された組織で業務を行うべきこと、秘密鍵の管理、業務の一時停止・終了に係る項目、他を規定
  - ファシリティの基準
    - 耐震・耐火基準、水害防止、電気設備、空調設備、他を規定
  - システム安全性の基準
    - 不正アクセス・攻撃等の検知・防御、不要な通信の遮断、システム可用性、全サーバの時刻同期、他を規定
  - 情報開示の基準
    - TSAポリシー（事業者情報、最大時刻差等）、問合せ窓口等の開示を規定

なお、ハッシュ関数の脆弱化、TSA公開鍵証明書を発行する認証事業者の廃業等、必要に応じ都度対応してきており、現時点で、大きな課題は無い。

※1 現行制度における審査を電子署名法にならい「調査」と表記、また、現行制度で規定する時刻認証業務の審査基準に沿った監査（内部監査でも可）を「監査」と表記している。

1. 調査・監査の内容

【調査の内容】

調査内容に関する議論を踏まえて

- 現行制度にない新たな観点
  - 事業体として求められる要件
    - 経理的基礎を求め、なおかつそれを審査項目として規定
- （参考）現行制度を基に整理・見直しが必要な項目
  - TSA自ら時刻の信頼性を確保する方式
  - 時刻認証業務の技術方式
  - HSMの要件
  - 認定の公表
  - 申請できる者の条件
  - その他

1. 調査・監査の内容

【監査の内容】

- 現状（タイムビジネス信頼・安心認定制度）
  - 審査基準全項目について実施
    - 年に1回以上、内部監査でも可
- EU※1
  - フル監査（調査内容）の50%を指標に、適格性の付与について何らかの影響を及ぼすような事態が発生していないことを確認する目的でサーベイランス監査を実施
    - 24か月毎のフル監査の間に1回、適合性評価機関による監査

※1 ETSI EN 319 403 適合性評価機関の要件 7.9 サーベイランス

適合性評価機関は、トラストサービスプロバイダーおよびその提供するトラストサービスが、継続して要件を満たしていることを確認するための現地監査を含む定期的なサーベイランスおよび再評価のプログラムを定義するものとする。フル監査の間に、少なくとも1年に1回のサーベイランスを実施することを推奨する。

※1 ㈱野村総合研究所によるTUV-IT社へのヒアリング結果（総務省委託事業）

1. 調査・監査の内容

論点について

- これまで検討会で示された方向性や議論等を踏まえ、調査の観点については、現行の制度における5つの観点に加え、「事業体の要件」を追加することで十分か。
- 監査の内容について、現行の制度では全項目を監査しているが、EUの実態も踏まえて内容を省略する余地はあるか。
- 監査の内容（新規・更新認定における全項目の確認）を省略する余地がある場合、どのような観点で省略する項目を検討することが適切か。

方向性に関する見解

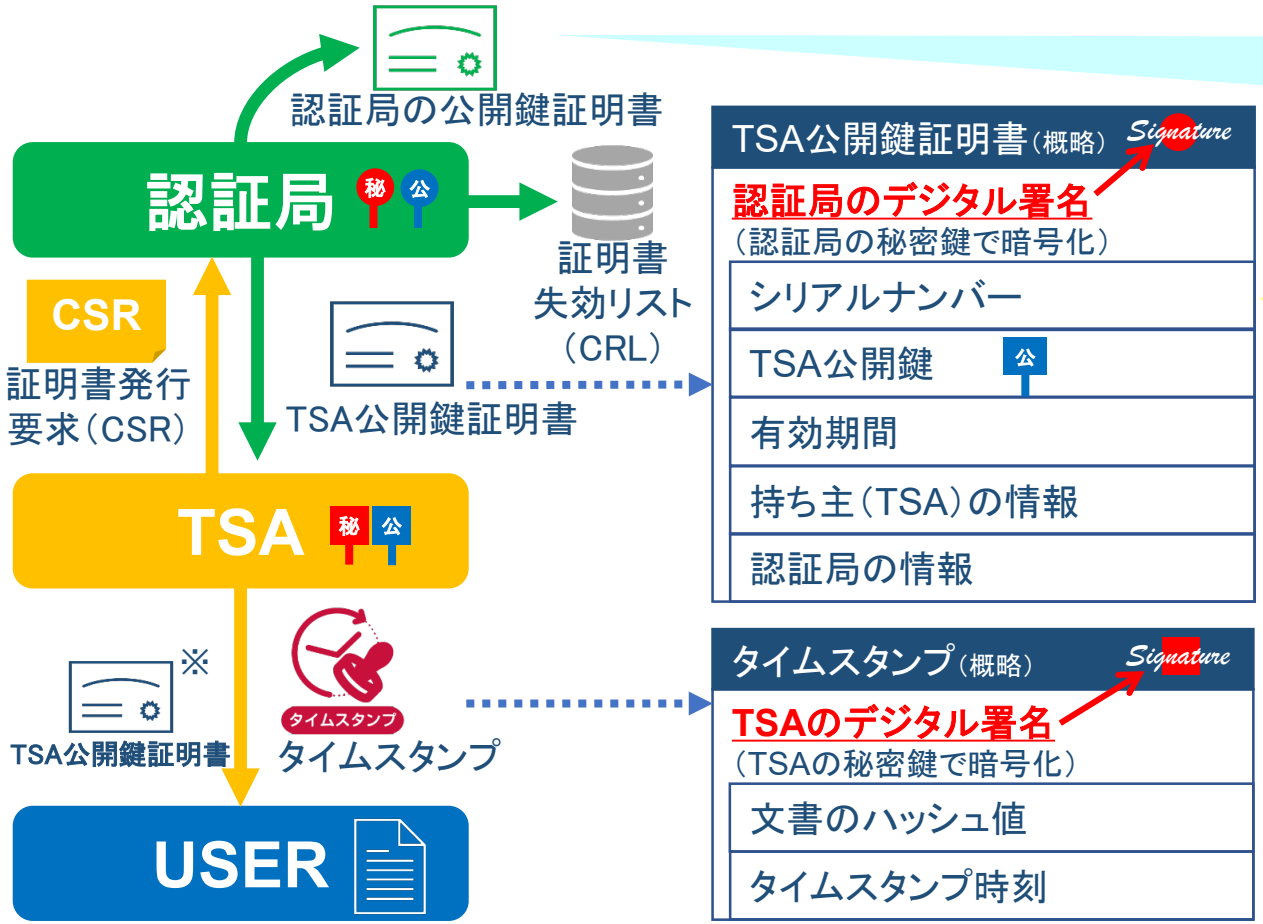
- 調査の観点については、現行の制度における5つの観点に加え、「事業体の要件」を追加することで十分ではないか。
- 内部監査でも可とする本制度においては、監査は全項目実施することが適当ではないか。

2. TSA公開鍵証明書を発行する認証事業者の基準

（参考）

TSA公開鍵証明書は、TSAの正当性を担保する電子証明書であり、正当な認証局が、TSAの実在確認、証明書発行要求の発出元確認を行い発行する。

・不当な認証局の場合、認定TSAの名を騙る「なりすまし」の証明書発行要求に応じてしまう惧れや、認証局の鍵管理が不十分で不正利用されてしまう惧れ等がある。



認証局の公開鍵証明書

・実際には、ルート認証局と中間認証局の2階層で構成されるケースが一般的。

・その場合、両認証局の証明書を検証、失効リストの確認を行う必要がある。

TSA公開鍵証明書（概略） Signature

認証局のデジタル署名
（認証局の秘密鍵で暗号化）

- シリアルナンバー
- TSA公開鍵 公
- 有効期間
- 持ち主（TSA）の情報
- 認証局の情報

TSA公開鍵証明書の検証

①認証局のデジタル署名の検証
正当な認証局が発行したTSA公開鍵証明書であることを確認

②失効リストの確認
タイムスタンプ発行時点でTSA公開鍵証明書が失効していなかったことを確認

タイムスタンプ（概略） Signature

TSAのデジタル署名
（TSAの秘密鍵で暗号化）

- 文書のハッシュ値
- タイムスタンプ時刻

タイムスタンプの検証

①ハッシュ値確認
対象文書（データ）に対するタイムスタンプであることを確認

②TSAのデジタル署名の検証
タイムスタンプ時刻等が改ざんされていないことを確認

※ TSA公開鍵証明書は別途リポジトリからダウンロードするケースもある

2. TSA公開鍵証明書を発行する認証事業者の基準

現状（タイムビジネス信頼・安心認定制度）

- 審査基準※1に、TSAに対し、選定すべきTSA公開鍵証明書を発行する認証事業者（CA）の基準を規定
  - 電子署名法の認定認証事業者と同等の厳密さで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監査を受けた認証事業者
- 実際に利用されている認証事業者
  - セコムトラストシステムズ（認定認証事業者, WebTrust※2）
    - アマノ、サイバーリンクス、TKCの3社が利用
  - GMOグローバルサイン（WebTrust）
    - セイコーソリューションズ、三菱電機インフォメーションネットワークの2社が利用

※1 **時刻認証業務審査基準　技術14. TSA公開鍵証明書を発行する認証事業者**

TSA公開鍵証明書に関して、以下の要件を満たすものであること
・電子署名法の規定に基づく認定認証事業者と同等の厳密さで秘密鍵を管理している認証事業者、または信頼のある監査機関から監査を受けた認証事業者であること
エビデンス例：運用規程、タイムスタンプトークン、CA局のCP/CPS、Web Trustに適合しているCAであることを示す資料

※2 米国公認会計士協会及びカナダ勅許会計士協会によって共同開発された電子商取引認証局監査プログラム

2. TSA公開鍵証明書を発行する認証事業者の基準

現状（タイムビジネス信頼・安心認定制度）

- 課題
  - 基準が不明確であり、TSAがCAを選定・判断することが困難
    - 電子署名法の規定に基づく認定認証事業者と**同等の厳密さで秘密鍵を管理**している認証事業者
      - エビデンスの提出等により当該基準を満たすかどうかを判断することは極めて困難
    - 信頼のある監査機関から監査を受けた認証事業者
      - 信頼のある監査機関について、審査基準のエビデンス例において「WebTrust」が例示されているのみで、他の監査について判断することは極めて困難
  - 認定認証事業者相当、もしくは、信頼ある監査機関から監査を受けた認証事業者であるとのTSAからの申請について、日本データ通信協会でその適合性を判断することが困難
    - 電子署名法の認定において現地調査が必須であり、エビデンス提出のみでは判断できない
    - 監査機関がどのような基準で、どのような実施方法で監査したのか判断できない
  - CAは、認定の対象外であり直接的な要件を求められず、実際にTSA公開鍵証明書を発行する体制・設備等の確認は出来ていない

2. TSA公開鍵証明書を発行する認証事業者の基準

EU

- ETSIが定める技術標準に、適格タイムスタンプの発行に用いる公開鍵証明書に関し、適格認証事業者によって発行されるべきことを規定※1

※1 ETSI EN 319 421 タイムスタンプを発行するTSPに対するポリシーとセキュリティ要件

8.1 TSA公開鍵証明書

タイムスタンプがeIDAS規則に従って適格な電子タイムスタンプであると主張されている場合、TSA公開鍵証明書は、ETSI EN 319 411-2証明書ポリシー下で動作する認証局（適格認証事業者）によって発行されなければならない。

原文：If a time-stamp is claimed to be a qualified electronic time-stamp as per Regulation (EU) No 910/2014 [i.4], the TSU signature verification (public) key certificate should be issued by a certification authority operating under ETSI EN 319 411-2 [i.11] certificate policy.

注）本要件は、「should」を用いて規定しているが、shouldの要件は、妥当な理由(Justification)がない限り適用されるものである。

2. TSA公開鍵証明書を発行する認証事業者の基準

論点について

- TSAがCAを選定・判断できるよう、TSA公開鍵証明書を発行するCAの基準を明確にすることが適切か。
- 明確にすることが適切である場合、その基準は電子署名法の認定認証事業者、または、WebTrust認証を受けた事業者であることを求めることが適切か。
- 電子署名法の認定やWebTrust認証以外に、他の認証制度や認定制度の活用の余地がある場合、どのような制度の活用が考え得るか。

方向性に関する見解

- TSAがCAを選定・判断できるよう、CAの基準を明確にすることが適切ではないか。
- その基準は、現行制度からのシームレスな移行を考慮し、電子署名法の認定認証事業者やWebTrustに適合した事業者であることを求めることが適当ではないか。

END

各論点について

タイムビジネス認定センター

参考）審査基準概要（1） ～デジタル署名方式TSA～

（1）技術基準

①タイムスタンプの時刻精度

・UTC(NICT)に対して±1秒以内であること

・時刻精度を満たしていないタイムスタンプの発行を防止する措置を講ずること

②タイムスタンプの時刻の精度の証明

・認定TAAからの時刻配信・監査を受けていること

③機器認証及び通信

・時刻配信・監査を受ける認定TAAの機器を特定し認証可能な手段を用いること

・利用者からタイムスタンプトークンの発行要求を受け付ける際には、時刻認証サービスの特定が可能な手段を用いること

・通信の暗号化を行うこと

④タイムスタンプトークンのデータ形式

・タイムスタンプトークンのデータ形式を明確に定義し、運用規定に記載・公開していること

⑤タイムスタンプトークンの生成に関わる暗号技術

・電子文書のハッシュ値を得るためのハッシュ関数やデジタル署名に用いる公開鍵暗号技術がCRYPTREC暗号リストの電子政府推奨暗号リストに記載されたものであること

⑥タイムスタンプトークンの生成に用いる秘密鍵の保護装置

・HSM（FIPS140-2のレベル3認証相当以上の製品）を用いて保護すること

参考）審査基準概要（2） ～デジタル署名方式TSA～

（1）技術基準（続き）

⑦TSA公開鍵証明書

・TSA用の公開鍵証明書であること（秘密鍵利用目的がタイムスタンプ発行であること）

・署名アルゴリズムがCRYPTREC暗号リストの電子政府推奨暗号リストに記載されたものであること

・TSA公開鍵証明書の発行日および有効期間の満了日が記載されていること

⑧TSA公開鍵証明書を発行する認証事業者

・電子署名法の規定に基づく認定認証事業者と同等の厳密さで秘密鍵を管理している認証事業者、または信頼のある監査機関からの監査を受けた認証事業者であること

・TSA公開鍵証明書を発行する認証局と、その発行に先立ち、認証局の認証業務終了に係る以下の事項について合意しておくこと

- 認証局は、時刻認証事業者が発行済みTSA公開鍵証明書に対応した秘密鍵を用いたタイムスタンプ発行を継続している間、認証業務を終了せず、当該公開鍵証明書に係る失効リストを最新の状態に保ち、またそれを公の状態に保つこと　他

⑨タイムスタンプトークンの生成処理

・耐タンパー性を有する装置等で生成処理を実装すること（例：HSM内での生成）、プログラム等の改ざん検知機能を有すること、他

⑩その他

参考）審査基準概要（3） ～デジタル署名方式TSA～

（2）運用基準

①組織・人事管理

- ・組織構成：独立性が確保された組織が時刻認証業務を担当すること
- ・専門性：時刻やセキュリティに関する専門性の優れた要員を配置すること
- ・事故を未然に防ぐために、部署内での内部牽制が働く組織構造・業務手順であること

②業務の一時停止・終了

- ・サービスの一時停止・終了時は、事前に手続きを決め利用者に通知すること
- ・障害発生時など予期できない場合の除き、事前の通知なしに業務を停止しないこと

③タイムスタンプトークン生成に用いる秘密鍵の管理

- ・秘密鍵の生成・廃棄：複数人管理のもと行うこと
- ・秘密鍵の保管：FIPS140-2のレベル3認証相当のHSM内に保管すること
- ・秘密鍵の危殆化時の対応：内部不正による秘密鍵の漏洩や第三者による秘密鍵の解読に備え、あらかじめ対応策を策定しておくこと

④その他

参考）審査基準概要（4） ～デジタル署名方式TSA～

（3）ファシリティの基準

①耐震基準：建築物の耐震性（建築基準法への適合性）、設備の耐震性

②耐火基準：建築基準法に規定する耐火建築物または準耐火建築物であること

③水害防止：システムの物理的配置等

④電気設備：無停電電源装置、バックアップ発電機等

⑤火災報知システム：自動火災報知機、消化装置の設置

⑥空調設備：温湿度管理ポリシー

⑦認定対象設備に対するアクセス：設置する場所、鍵付ラック、入退室管理等

（4）システム安全性の基準

①外部ネットワークとの接続：外部ネットワークからの不正アクセス・攻撃等の検知・防御

②内部ネットワーク：サーバ等を適切に配置し不要な通信を遮断すること。ネットワーク機器のセキュリティ更新

③サーバ・ストレージ：不要アクセスの拒否、不要アプリケーションの削除、不要ポートの利用停止等

④システムの可用性：システムの障害に備えたサービス継続のための対策

③システムの時刻：ログを残す全てのサーバは十分な精度で時刻同期出来ていること

参考）審査基準概要（５） ～デジタル署名方式TSA～

（５）情報開示の基準

①TSAポリシーの公開

・事業者情報、UTCとの最大時刻差、TAAとのポリシーリンク

・タイムスタンプトークンのデータ形式、有効期間、他

②利用者および利用者に関わる関係者への情報開示

・問い合わせ窓口情報、時刻監査情報、他

③加入者への通知・連絡

・サービスの一時停止・終了時の通知、システムトラブル等の発生時の通知