資料１－３

第1回 タイムスタンプ認定制度に関する検討会

タイムビジネス信頼・安心認定制度について

2020年3月30日

タイムビジネス認定センター長
伊地知　理

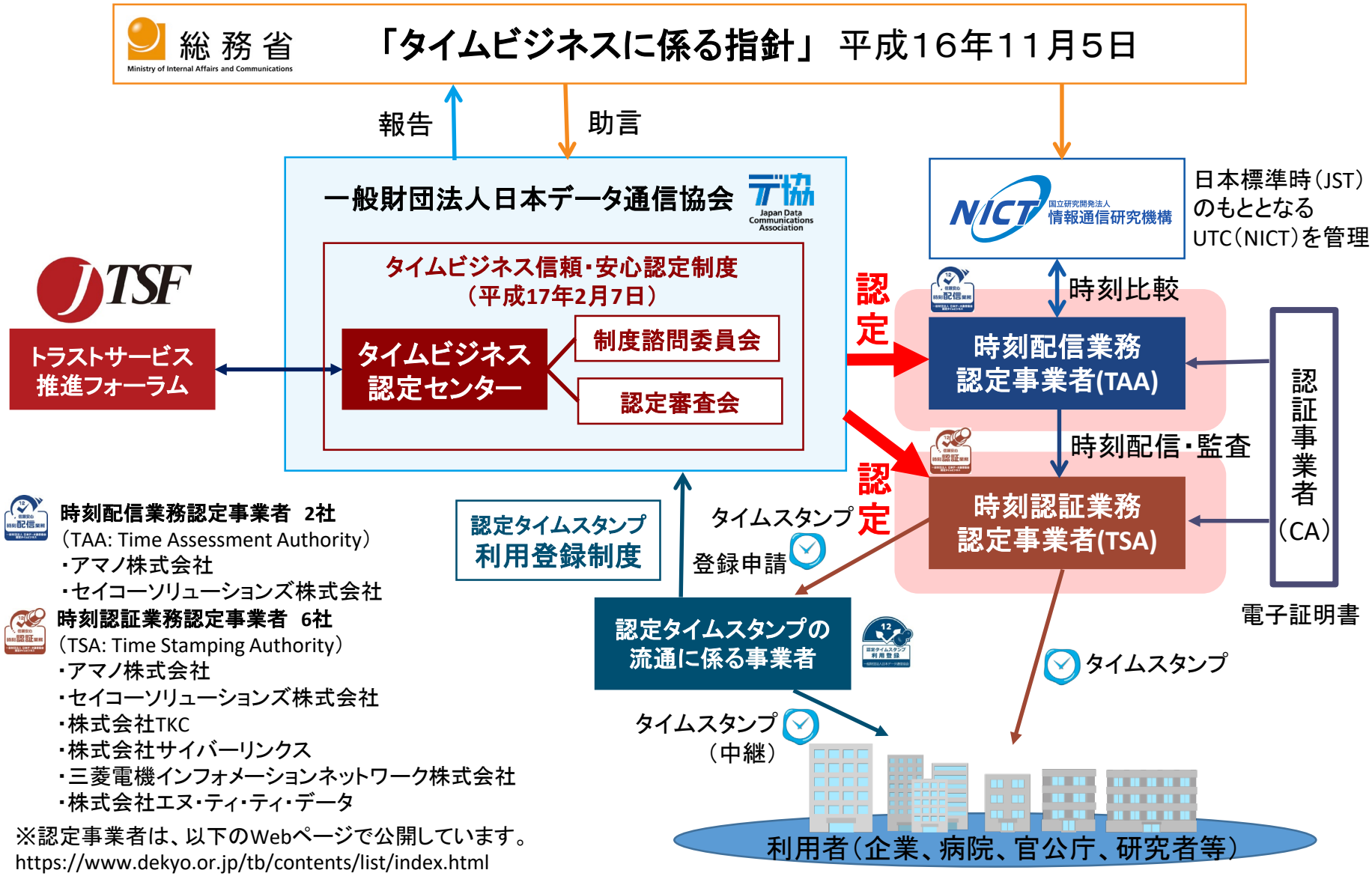
一般財団法人
日本データ通信協会

目次

1. タイムビジネスの仕組み
2. デ協の制度の枠組み
3. デ協の審査基準

1. タイムビジネスの仕組み
2. デ協の制度の枠組み
3. デ協の審査基準

タイムビジネスの仕組み



時刻配信業務認定事業者　2社
（TAA: Time Assessment Authority）
・アマノ株式会社
・セイコーソリューションズ株式会社

時刻認証業務認定事業者　6社
（TSA: Time Stamping Authority）
・アマノ株式会社
・セイコーソリューションズ株式会社
・株式会社TKC
・株式会社サイバーリンクス
・三菱電機インフォメーションネットワーク株式会社
・株式会社エヌ・ティ・ティ・データ

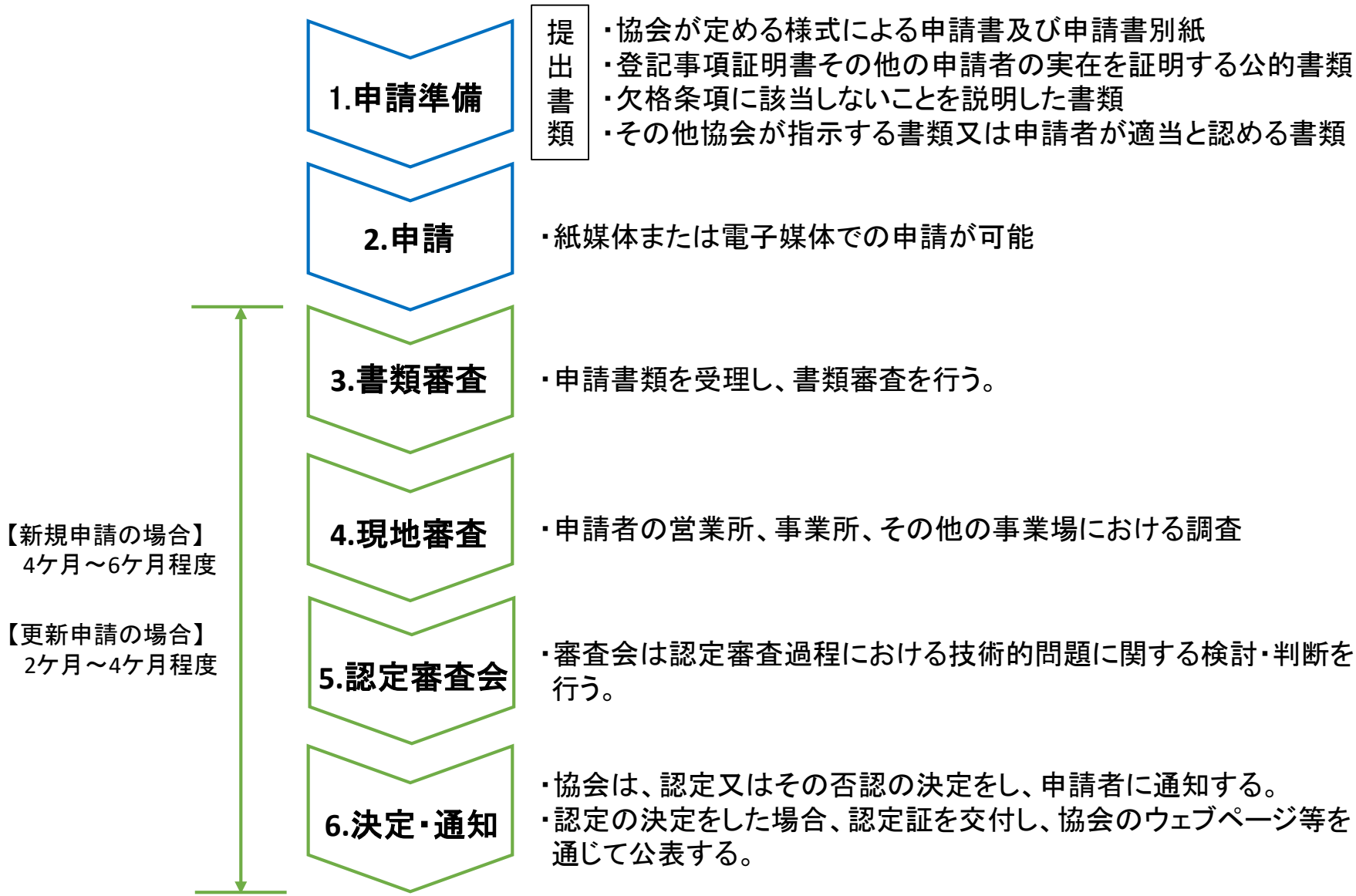
※認定事業者は、以下のWebページで公開しています。
https://www.dekyo.or.jp/tb/contents/list/index.html

1. タイムビジネスの仕組み
2. デ協の制度の枠組み
3. デ協の審査基準

制度概要

1.名称	タイムビジネス信頼・安心認定制度
2.運営主体	一般財団法人日本データ通信協会
3.制度開始	平成17年（2005年）2月7日
4.認定に係る業務	• 時刻配信業務 • 時刻認証業務（デジタル署名を使用する方式、リンキング方式、アーカイビング方式）
5.審査基準	タイムビジネスに係る指針を踏まえ当協会が策定
6.認定	審査基準への適合性を評価することにより認定する
7.認定の有効期間	認定の日から2年
8.監査の報告	認定事業者は、年一回以上の監査を行い、当該監査の結果を協会に報告しなければならない
9.報告義務	タイムビジネスの信頼性又は安心性を損なうおそれがある緊急事態について報告義務がある
10.業務廃止の届出	業務を廃止したときは、遅滞なく協会に届け出る必要がある
11.認定審査会	認定審査過程における技術的問題に関する検討・判断
12.制度諮問委員会	認定制度の企画立案及び運用に関する重要事項について審議

申請から認定までの流れ



1. タイムビジネスの仕組み
2. デ協の制度の枠組み
3. デ協の審査基準

適合性評価の観点と審査基準の種類

適合性評価の観点

（1）技術基準
（2）運用基準
（3）ファシリティの基準
（4）システム安全性の基準
（5）情報開示の基準

審査基準の種類

時刻配信業務
審査基準

2事業者

審査基準の改正等にあたっては、
制度諮問委員会に諮問する。

時刻認証業務 審査基準 （デジタル署名 を用いる方式）	時刻認証業務 審査基準 （リンキング方式）	時刻認証業務 審査基準 （アーカイビング 方式）
5事業者	なし	1事業者

3つの技術方式

審査基準　ピックアップ紹介（1）

TAA
TSA

■デジタル署名を用いる方式
■リンキング方式
■アーカイビング方式

（1）技術基準
（2）運用基準
（3）ファシリティの基準
（4）システム安全性の基準
（5）情報開示の基準

TAA時計の構成
TAA時計の精度

審査基準

（1）技術基準　＞　技術要件全般（JIS X 5094:2019）　＞　TAA時計の要件　＞　TAA時計の構成

- TAA時計※1は、基準時計※2、時刻監査機器及び時刻配信機器で構成しなければならない。

（1）技術基準　＞　技術要件全般（JIS X 5094:2019）　＞　TAA時計の要件　＞　TAA時計の精度

- 基準時計は、UTC（NICT）※3に対して±5ミリ秒以内で同期していること。

※1　TAAの技術基準は、JIS X 5094（UTCトレーサビリティ保証のためのタイムアセスメント機関(TAA)の技術要件）の一部を指定しており、JISにおいて、TAA時計は、時刻監査及び時刻配信において使用するTAAの時計システムと定義されています。
※2　各時刻配信事業者は、基準時計としてルビジウム原子時計等の設備を有しています。
※3　UTCは協定世界時と呼ばれるもので、世界各国の機関が原子時計の時刻を比較し決定している。各機関（k）が運用する時刻はUTC（k）と表記され、NICTが運用する時刻はUTC（NICT）となる。デ協基準ではUTC（NICT）との同期を求めているが、国際標準では、UTCを運営する機関を特定せずUTC（k）との同期を求めている。

審査基準　ピックアップ紹介（2）

Japan Data Communications Association

TAA
TSA

■デジタル署名を用いる方式
■リンキング方式
■アーカイビング方式

（1）技術基準
（2）運用基準
（3）ファシリティの基準
（4）システム安全性の基準
（5）情報開示の基準

TSA時計の時刻異常への対応

審査基準

（1）技術基準＞技術要件全般（JIS X 5094:2019）＞時刻監査の要件＞TSA時計の時刻異常への対応

- TSA時計※1の時刻異常を検知した場合、関連TSAに通知すること※2

（1）技術基準＞ TSA時計の時刻異常への対応

- TSAのタイムスタンプ発行機能を停止する機能を用いてもよい※3

※1　タイムスタンプトークンに含まれる時刻を生成するタイムスタンプサーバの時計
※2　JIS X 5094（UTCトレーサビリティ保証のためのタイムアセスメント機関(TAA)の技術要件）では、TAAがTSAの時刻異常を検知した場合には、時刻異常が生じているTSAに通知することを求めています。
※3　デ協の審査基準では、JIS X 5094の前述の規定に加えて、TSAのタイムスタンプ発行機能を停止する機能を用いることも認めています。

審査基準　ピックアップ紹介（3）

TAA
TSA

■デジタル署名を用いる方式
■リンキング方式
■アーカイビング方式

（1）技術基準
（2）運用基準
（3）ファシリティの基準
（4）システム安全性の基準
（5）情報開示の基準

時刻精度
時刻精度の証明

審査基準

（1）技術基準　＞　精度

- タイムスタンプの時刻は、UTC（NICT）に対して±1秒以内であること※1

（1）技術基準　＞　精度の証明　＞　認定を受けたTAAからの時刻配信／認定を受けたTAAによる時刻監査

- 認定TAAからの時刻配信・監査を受けていること※2

（1）技術基準　＞　タイムスタンプトークンの時刻の品質　＞　時刻の品質の管理

- 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※3

※1　TAAの技術要件を定めたJIS X 5094において、「TSTに含まれる時刻の値がUTC（k）の±1秒で正確であること」という考え方が示されています。
※2　プラットフォームサービスに関する研究会　トラストサービス検討ワーキンググループ　最終とりまとめに記載の「時刻配信業務の扱い」と密接に関係する項目です。
※3　TSAは、TAAからの時刻監査とは別に、TSA独自の仕組みにおいて、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じています。

審査基準　ピックアップ紹介（4）

TAA
TSA

■デジタル署名を用いる方式
■リンキング方式
■アーカイビング方式

（1）技術基準
（2）運用基準
（3）ファシリティの基準
（4）システム安全性の基準
（5）情報開示の基準

組織・人事管理

審査基準

（2）運用基準　＞　組織・人事管理　＞　組織構成

- 独立性が確保された組織で業務を行うこと※1

（2）運用基準　＞　組織・人事管理　＞　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。また適切な業務運営が行われるための教育訓練を行うこと

（2）運用基準　＞　組織・人事管理　＞　内部牽制機能

- 事故を未然に防ぐために、部署内での内部牽制が働く構造、業務手順になっていること

※1　他部門からの干渉・拘束等により要員が軋轢に屈し、不正なタイムスタンプが発行されること等がないよう、組織としての独立性の確保が求められています。（企業の内部監査部門等と同様に、認定業務運用部門にも他部門からの不当な介入を受けないよう、組織としての独立性の確保がが求められています）。

審査基準　ピックアップ紹介（5）

TAA
TSA

■デジタル署名を用いる方式
■リンキング方式
■アーカイビング方式

（1）技術基準
（2）運用基準
（3）ファシリティの基準
（4）システム安全性の基準
（5）情報開示の基準

秘密鍵の管理

審査基準

（2）運用基準　＞　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

- 秘密鍵の生成は、信頼できる鍵生成システムを利用し※1、複数人管理のもとで行うこと

（2）運用基準　＞　タイムスタンプトークン生成に用いる秘密鍵の管理　＞　秘密鍵の保管

- 鍵生成システムによって生成された秘密鍵は、HSM※2（FIPS140-2のレベル3※3認証相当以上の製品※4）内に保管すること

※1　秘密鍵は、タイムスタンプ発行に用いる暗号鍵。この秘密鍵を生成する鍵生成システムにセキュリティ上の欠陥があった場合、鍵が解読され、タイムスタンプが偽造される危険性があります。

※2　HSM（Hardware Security Module）は、耐タンパー機構による物理的な安全性が確保された鍵管理機能を備えた暗号処理装置。一般に、鍵の生成やデジタル署名の生成等の機能も備えています。

※3　FIPS 140（Federal Information Processing Standardization 140）は、暗号モジュールに関するセキュリティ要件の仕様を規定する米国連邦標準規格。FIPS 140-2は2001年5月25日に発行され、FIPS 140-3が2019年3月22日に発行されています。

※4　デ協基準では、FIPS140-2レベル3認証相当のHSMを用いることを求めていますが、ETSIの定める要件では、複数の国際基準（ISO/IEC 15408, 19790等）が示され、いずれかに適合することを求めています。

審査基準　ピックアップ紹介（6）

TAA
TSA

■デジタル署名を用いる方式
■リンキング方式
■アーカイビング方式

（1）技術基準
（2）運用基準
（3）ファシリティの基準
（4）システム安全性の基準
（5）情報開示の基準

建築物の耐震性
外部ネットワークとの接続
ポリシーの公開

審査基準

（3）ファシリティの基準　＞　耐震基準　＞　建築物の耐震性

- 業務用設備を含む建築物は「地震に対する安全性に係る建築基準法」またはこれに基づく命令、条例の規定に適合するものであること

（4）システム安全性の基準　＞　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、攻撃等に対し、それを検知および防御するためのシステム（ファイアウォール等）を備え、必要に応じてセキュリティ更新がなされること

（5）情報開示の基準　＞　ポリシーの公開　＞　サービス利用規約

- 事業者が定めるサービス利用規約を明記
- サービス利用に係る注意事項があれば明記

参考：審査基準概要

審査基準概要（1）TAA

（1）技術基準

技術要件全般は、JIS X 5094:2019（UTCトレーサビリティ保証のためのタイムアセスメント機関（TAA）の技術要件）の一部を引用している。（※本資料はJIS規定内容を要約し記載しています）

①TAA時計の構成【JIS】

・TAA時計は、基準時計、時刻監査機器及び時刻配信機器で構成しなければならない

②TAA時計の精度【JIS】

・基準時計の精度：UTC(NICT)に対して±5ミリ秒以内で同期していること

③時刻差の測定及び測定データの保存【JIS】

・TAAは、GPSコモンビュー法又は相当の方式によって、UTC(NICT)と基準時計との時刻差を計測し、測定データを保存しなければならない

④TSA時計の時刻異常への対応

・TSA時計の時刻異常を検知した場合、関連TSAに通知すること【JIS】

・TSAのタイムスタンプ発行機能を停止する機能を用いること（してもよい）【デ協】

⑤通信に用いる暗号技術

・電子政府における調達のために参照すべき暗号のリスト（CRYPTREC暗号リスト）の電子政府推奨暗号リストに記載された暗号技術を用いること【デ協】

審査基準概要（2）TAA

（2）運用基準

①組織・人事管理

・独立性が確保された組織で業務を行うこと、専門性の優れた要員を配置すること、内部牽制が働く組織構造であること、他

②業務の一時停止・終了

・業務の一時停止や終了時の通知手順等に関する事項、予告なしの業務停止の禁止、他

③その他：業務監査、システムのトラブル・災害からの復旧、他

（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

審査基準概要（3）TAA

（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

（5）情報開示の基準

①TAAポリシーの公開

・事業者情報、UTCとの最大時刻差、UTC(NICT)とのポリシーリンク※1、他

②加入者および加入者に関わる関係者への情報開示

・問い合わせ窓口情報、UTC(NICT)との時刻差の実測データ、経営情報、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

※1）UTC(NICT)とのポリシーリンク
TAAによるNICTとの時刻比較に関し、比較対象となるNICTの時刻比較データを一意に示すために、NICTの時刻比較データ公開ポリシーOID等をTAAの運用規定に明記することを指す。

審査基準概要（4）TSA（デジタル署名方式）

Japan Data Communications Association

（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

審査基準概要(5) TSA(デジタル署名方式)

(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

審査基準概要（6）TSA（デジタル署名方式）

（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

審査基準概要（7）TSA（デジタル署名方式）

（3）ファシリティの基準　（TAA審査基準に同じ）

（4）システム安全性の基準（TAA審査基準に同じ）

（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

審査基準概要（8）TSA（リンキング方式・アーカイビング方式）

（1）技術基準

TSA-D（デジタル署名方式）審査基準に加え以下の項目等が規定されている。

①照合用データの保管処理：保管処理のプログラムが正しく実装されていること（当該方式は、タイムスタンプに係る情報をTSAが安全に保管することが重要であるため）

②照合用データの完全性：照合用データの完全性が証明できること。情報の書換え、順序変更、挿入、削除などの変更操作ができないか、または変更操作が行われた場合には確実に検知できる方式で記録されること。

※タイムスタンプトークン生成に秘密鍵は用いないため、秘密鍵に関する基準はない

（2）運用基準

TSA-D（デジタル署名方式）審査基準に加え以下の項目等が規定されている。

①照合用データの保管を行うプログラム等の変更および操作

・プログラムに変更を加える場合には、変更内容について認定機関に提示しチェックを受けること。

②照合用データの管理

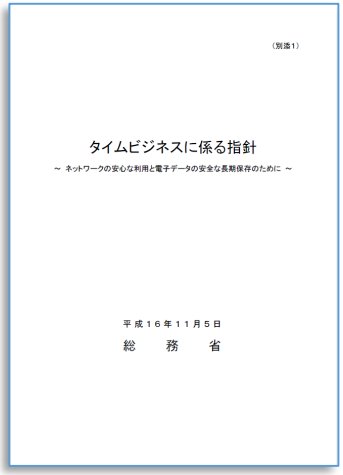
・タイムスタンプトークン照合用データを保持し、その完全性を維持すること、他

※（3）ファシリティの基準、（4）システム安全性の基準、（5）情報開示の基準

・TSA-D（デジタル署名方式）に同じ

参考

（参考）タイムビジネスに係る指針（平成16年11月5日）


（別添1）

タイムビジネスに係る指針

～ ネットワークの安心な利用と電子データの安全な長期保存のために ～

平成16年11月5日

総　務　省

- タイムビジネス
  - 「時刻配信業務」及び「時刻認証業務」の総称を指す。
- 時刻配信業務
  - 情報通信ネットワークを利用する上で必要となるサーバ等の電気通信設備に用いられる時刻に高い信頼性を与えるため情報通信ネットワークを通じて時刻情報を配信する業務、更に配信先の時刻精度を計測して報告を行う時刻監査業務をいう。
- 時刻認証業務
  - 電磁的記録に記録された情報（以下「電子データ」という。）に係る情報について行われる措置であるタイムスタンプの付与及び当該タイムスタンプの有効性を証明する業務をいう。
- タイムスタンプ
  - 電子データがある時刻に存在していたこと及びその時刻以降に当該電子データが改ざんされていないことを証明できる機能を有する時刻証明情報。
- 標準時
  - 独立行政法人情報通信研究機構法（平成１１年法律第１６２号）第１３条第１項第３号に基づき、独立行政法人情報通信研究機構が通報する標準時を指す。
  - なお、時刻配信業務のうち、標準時に準拠した時刻情報を配信する業務を特に標準時配信業務という。

（参考）申請書

❶新規

年　月　日

一般財団法人日本データ通信協会
タイムビジネス認定センター　殿

タイムビジネス信頼・安心認定申請書

＿＿＿＿＿＿業務につき、タイムビジネス信頼・安心認定を受けたいので、タイムビジネス信頼・安心認定制度運用規約第６条１項の規定により、別紙の通り申請します。

事業者名称		
ＵＲＬ		
代表者氏名（ふりがな）		印
住所：	〒	
代表 TEL：		
担当部署：		
申請担当者：		
TEL：		
FAX：		
e-mail：		

注）当協会は、個人情報を申請者からの申し出に基づき正確な状態で管理します。

※本欄は協会処理欄となりますので、記入しないで下さい。

受付日	申請書類確認	入金確認日	書類審査合・否	現地審査合・否
認定証の発送	認定日		認定番号	

❷更新

年　月　日

一般財団法人日本データ通信協会
タイムビジネス認定センター　殿

タイムビジネス信頼・安心認定更新申請書

＿＿＿＿＿＿業務（認定番号：　　）につき、タイムビジネス信頼・安心認定の更新（変更を含む、変更を含まない）を受けたいので、タイムビジネス信頼・安心認定制度運用規約第１６条２項の規定により、別紙の通り申請します。

❸変更

年　月　日

一般財団法人日本データ通信協会
タイムビジネス認定センター　殿

タイムビジネス信頼・安心認定業務内容変更申請書

＿＿＿＿＿＿業務（認定番号：　　）につき、認定に係る業務内容に関する事項の変更認定を受けたいので、タイムビジネス信頼・安心認定制度運用規約第17条の規定により、別紙の通り申請します。

事業者名称		
ＵＲＬ		
代表者氏名（ふりがな）		印
住所：	〒	
代表 TEL：		
担当部署：		
申請担当者：		
TEL：		

（参考）申請書別紙

例）デジタル署名を使用する方式

1ページめ

2019.06.19 改正（2019.06.19施行）

タイムビジネス信頼・安心認定　申請書別紙
（時刻認証業務：デジタル署名を使用する方式）

タイムビジネス信頼・安心認定　申請書別紙
（時刻認証業務：デジタル署名を使用する方式）
2019年6月19日改正（2019年6月19日施行）

申請事業者名：　〇△■＊株式会社

申請サービス名：〇△■＊タイムスタンプサービス

作成日：

2ページめ

2019.06.19 改正（2019.06.19施行）

タイムビジネス信頼・安心認定　申請書別紙
（時刻認証業務：デジタル署名を使用する方式）

項目　基準（遵守事項）　説明資料　資料番号

（1）　技術基準

項目	基準（遵守事項）	説明資料	備考（措置状況の補足説明）	資料番号
1　タイムスタンプトークンの時刻	タイムスタンプトークンに含まれる時刻は、TSA時計により生成されること			
2　精度	TSA時計は、認定TAAから時刻配信を受け、UTC（NICT）に対し±1秒以内で同期していること			
3　精度の証明	TSA時計の品質を証明する手段を持つこと			
1　認定を受けたTAAからの時刻配信	第三者もしくは時刻認証業務とは権限分離された組織が運営し、時刻配信業務についてタイムビジネス信頼・安心認定を受けたTAAから時刻配信を受けていることを証明できること			
2　認定を受けたTAAによる時刻監査	第三者もしくは時刻認証業務とは権限分離された組織が運営し、時刻配信業務についてタイムビジネス信頼・安心認定を受けた機関がTAAとしてTSA時計の時刻監査を行っていることを証明できること			
4　タイムスタンプサービス等の特定	タイムスタンプサービス等を特定する手段および、なりすまし対策を講じること			
1　時刻配信を受ける機器の特定（TAA-TSA間）	時刻配信を受けるTAAの配信元機器の特定および認証可能な手段を用いること			
2　タイムスタンプサービスの特定（利用者→TSA）	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			

備考（措置状況の補足説明）

(参考)審査基準

例)デジタル署名を使用する方式

2019.06.19改正（2019.06.19 施行）　時刻認証業務審査基準(デジタル署名を使用する方式)

1ページめ

一般財団法人日本データ通信協会
タイムビジネス認定センター

時刻認証業務審査基準（デジタル署名を使用する方式）

2019年6月19日改正（2019年6月19日施行）

[定義]
デジタル署名を使用する方式の時刻認証サービスとは、時刻認証局（TSA）がタイムスタンプトークンを生成する際、信頼できる電子認証局(CA)により公開鍵証明書の発行を受けた専用の暗号鍵（デジタル署名に用いる暗号鍵に限定される場合には、以下秘密鍵と記す。）を用いて各タイムスタンプトークンにデジタル署名を施すことによってタイムスタンプトークンの信頼性を確保する方式である。
デジタル署名を使用する方式の時刻認証サービスでTSA
ンのデジタル署名に用いる秘密鍵の公開鍵証明書（TSA
ンプトークンに対し、指定された署名アルゴリズムで

タイムスタンプ検証の際は、①タイムスタンプ付与対
証、という一連の手順を実行することにより検証を行

本方式では、タイムスタンプ検証の信頼性は、各タイ
た秘密鍵を用いてタイムスタンプトークンにデジタル
とが求められる。

関連する標準： ISO/IEC18014-1、ISO/IEC18014-2、RF

関連用語の定義
TSA公開鍵証明書
デジタル署名を用いる方式のタイムスタンプトークン
の秘密鍵に対応した公開鍵を証明する公開鍵証明書を
期間、証明書の失効確認先情報が含まれ、CAがデジタ

検証
タイムスタンプトークン保有者が、タイムスタンプト
る。

1．ハッシュ値確認：タイムスタンプ付与対象文書の
2．デジタル署名の検証：TSA公開鍵を用いてタイムス
3．TSA公開鍵証明書失効確認：ルートCAに至るまでの

耐タンパー性
耐タンパー性とは、機密情報を保護しているハードウ
ンプラなどで解析できない仕組みを備えたソフトウェ
代表的なハードウェアとして米国政府が定めたFIPS140

耐タンパー性を有する装置(装置：ここではハードウェ
1．内部の情報が外部に不正なアクセスで漏洩しない
2．内部の情報が外部から不正なアクセスで改ざんで
3．内部の機能が外部から不正なアクセスで改変でき

2019.06.19改正（2019.06.19 施行）　時刻認証業務審査基準(デジタル署名を使用する方式)

2ページめ

HSM
ハードウェアセキュリティモジュール（Hardware Security Module：HSM）とは、耐タンパー機構による物理的な安全性が確保された鍵管理機能を備えた暗号処理装置。PCIバス仕様のモジュールおよびICカード等による暗号処理等の機密性が物理的に保護されている。具体的な耐タンパー機構としては、装置本体の内部を分解したり、衝撃を加えたりすると装置内の重要なデータが自動的に消失されるものや温度や気圧の変化等々の環境変化でも重要なデータが自動的に消失される仕掛けになっている。耐タンパー機構や安全対策レベル等々については、米国政府が定めたFIPS140-2の基準があり、審査登録機関による適切な審査と認証が行われている。

HSMが具備すべき要件は以下の通りである。
1．内部の情報が外部に不正なアクセスで漏洩しないこと
2．内部の情報が外部から不正なアクセスで改ざんできないこと
3．内部の機能が外部から不正なアクセスで改変できないこと
4．上記安全性が公的な審査登録機関により認証が与えられていること

FIPS 140-2
Federal Information Processing Standard 140-2 。米国NISTが策定した暗号モジュールに関するセキュリティ基準。最低レベル１から最高レベル4までである。

TSA時計
タイムスタンプトークンに含まれる時刻を生成するタイムスタンプサーバの時計

時刻ソース
TSAが時刻源として参照している認定TAAの時計

運用規程
TSAが公開する時刻認証業務についての基本的内容（ポリシー）と運用に関する基本的事項を明記した文書。TPS又はTP/TPSと表現されている場合もある。

利用者
TSAにタイムスタンプトークン発行要求を出してタイムスタンプトークンを受け取る者。タイムスタンプトークンを用いたアプリケーションサービスを行う事業者は利用者である。

検証者
タイムスタンプトークンの有効性確認を実施しようとする者

項目　基準(遵守事項)　エビデンス例

（１）　技術基準

項目	基準（遵守事項）	エビデンス例
1　タイムスタンプトークンの時刻	タイムスタンプトークンに含まれる時刻は、TSA時計により生成されること	運用規程 TSA時計に関した技術資料
2　精度	TSA時計は、認定TAAから時刻配信を受け、UTC（NICT)に対し±1秒以内で同期していること	運用規程 時刻監査記録
3　精度の証明	TSA時計の品質を証明する手段を持つこと	
1　認定を受けたTAAからの時刻配信	第三者もしくは時刻認証業務とは権限分離された組織が運営し、時刻配信業務についてタイムビジネス信頼・安心認定を受けたTAAから時刻配信を受けていることを証明できること	運用規程 TAAとの契約書類 リポジトリ情報
2　認定を受けたTAAによる時刻監査	第三者もしくは時刻認証業務とは権限分離された組織が運営し、時刻配信業務についてタイムビジネス信頼・安心認定を受けた機関がTAAとしてTSA時計の時刻監査を行っていることを証明できること	運用規程 時刻監査記録 TAAとの契約書類 タイムスタンプトークン（TACを含む場合） リポジトリ情報

（参考）申請料金

項目		金額
申請料	新規	2,000,000円
	更新	1,523,809円
	変更	428,571円
交通費及び宿泊費等		実費
追加調査費（一日あたり） ※現地審査が二日を超える場合		171,428円

※消費税別

END

タイムビジネス信頼・安心認定制度について

2020年3月30日

一般財団法人日本データ通信協会

タイムビジネス認定センター