時刻認証業務（デジタル署名を使用する方式）

[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が発行するタイムスタンプトークンには、タイムスタンプ付与対象文書のハッシュ値、タイムスタンプ付与時刻、タイムスタンプトークンのデジタル署名に用いる秘密鍵の公開鍵証明書（TSA公開鍵証明書）またはその入手先情報、使用するデジタル署名の署名アルゴリズムや鍵長に関する情報が含まれ、また、当該タイムスタンプトークンに対し、指定された署名アルゴリズムで生成したデジタル署名が付与される。

タイムスタンプ検証の際は、①タイムスタンプ付与対象文書のハッシュ値確認、②タイムスタンプトークンに付与されたデジタル署名の検証、③TSA公開鍵証明書失効確認を含む証明書パス検証、という一連の手順を実行することにより検証を行う。検証は、タイムスタンプ保有者がTSAに依存することなく実行可能でなければならない。

本方式では、タイムスタンプ検証の信頼性は、各タイムスタンプトークンに付与するデジタル署名の信頼性に依存している。したがって、TSAは信頼できるCAにより公開鍵証明書の発行を受けた秘密鍵を用いてタイムスタンプトークンにデジタル署名を施すこと、十分な安全性を有する署名アルゴリズムとハッシュ関数を用いること、デジタル署名に用いる秘密鍵を厳重に管理することが求められる。

関連する標準： ISO/IEC18014-1、ISO/IEC18014-2、RFC3161

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を発行するTSAは、この目的のための専用の秘密鍵を用いてタイムスタンプトークンにデジタル署名を付与しなければならない。この専用の秘密鍵に対応した公開鍵を証明する公開鍵証明書をTSA公開鍵証明書と呼ぶ。TSA公開鍵証明書には、当該公開鍵のほか、対象のTSAに関する情報、証明書を発行するCAの情報、公開鍵の有効期間、証明書の失効確認先情報が含まれ、CAがデジタル署名を付与する。

検証
タイムスタンプトークン保有者が、タイムスタンプトークンが真正で有効であることを確認するための一連の行為を指す。デジタル署名を使用する方式の検証は次の３つのプロセスで構成される。

１．ハッシュ値確認：タイムスタンプ付与対象文書のハッシュ値を計算し、タイムスタンプトークンに含まれるハッシュ値との一致を確認するプロセス
２．デジタル署名の検証：TSA公開鍵を用いてタイムスタンプトークンに付されたデジタル署名を復号し、タイムスタンプトークンから再計算したハッシュ値との整合性を確認するプロセス
３．TSA公開鍵証明書失効確認：ルートCAに至るまでの証明書の整合性検証や、TSA公開鍵証明書・中間CAの証明書が失効していないことをCAに問い合わせ確認するプロセス

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ェアやソフトウェアなどが、外部からの解析が困難な仕組みを備えた防護力を言う。具体的な耐タンパー性を有する機構としては、逆アセンブラなどで解析できない仕組みを備えたソフトウェアや、ハードウェア本体の内部を分解したり、衝撃を加えたりすると内部の重要なデータが自動的に消失されるハードウェアなどがある。代表的なハードウェアとして米国政府が定めたFIPS140-2の基準に適合したHSMがある。

耐タンパー性を有する装置(装置：ここではハードウェア、ソフトウェア、ファームウェア、もしくはその組合せと定義する)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

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

（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
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	

<table>
<tr><th>項目</th><th>基準（遵守事項）</th><th>エビデンス例</th></tr>
<tr><td>１ 時刻配信を受ける機器の特定（TAA-TSA間）</td><td>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</td><td>時刻配信時の特定方法を説明する資料
例：TAAとの契約時の申請フォーマット、TAAの時刻監査報告、トークンなど</td></tr>
<tr><td>２ タイムスタンプサービスの特定（利用者→TSA）</td><td>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</td><td>サービスを特定する方法についての資料</td></tr>
<tr><td>５　安全な通信路</td><td>時刻認証業務に係る通信では、セキュリティ対策がなされていること</td><td></td></tr>
<tr><td>１ TAA-TSA間</td><td>TAA-TSA間の通信はセキュリティ対策（なりすまし、改ざん、暗号化の対策など）がなされていること</td><td>技術仕様書
利用契約書類</td></tr>
<tr><td>２ TSA-利用者間</td><td>利用者とTSAの通信はセキュリティ対策（なりすまし、改ざん、暗号化の対策など）がなされていること</td><td>技術仕様書
利用契約書類</td></tr>
<tr><td>３ 暗号技術</td><td>時刻認証業務の通信路の安全性を公開鍵暗号技術または共通鍵暗号技術により実現する場合、電子政府における調達のために参照すべき暗号リスト（CRYPTREC暗号リスト）（平成25年3月1日に総務省、経済産業省が公表したもの）において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。ただし、2015年1月1日以前に認定された事業者においては、SHA-1については、SSL3.0、TLS1.0/1.1/1.2、VPN、およびTSAが利用者識別に用いるCMS署名ならびに時刻配信監査時の認証、改ざん検知に用いるHMACにおいて互換性維持のために利用することを当面可とする。また、128-bit RC4については、SSL(TLS1.0以上）での利用を当面認める。</td><td>運用規程
安全性レベルの証明資料</td></tr>
<tr><td>６　タイムスタンプトークンのTSAポリシーへのリンク</td><td>タイムスタンプトークンには、TSAポリシーの識別情報、リファレンス情報、ハッシュ値など、TSAポリシーを一意に特定できる情報を含めること</td><td>運用規程
タイムスタンプトークン
オブジェクトIDの割り当てに関する説明資料など</td></tr>
<tr><td>７　タイムスタンプトークンのデータ形式</td><td>タイムスタンプトークンのデータ形式を、明確に定義し、運用規程に記載・公開していること</td><td>運用規程
タイムスタンプトークン</td></tr>
<tr><td>８　タイムスタンプトークンに含むべき情報</td><td>以下の情報をタイムスタンプトークンに含めること（〇は必須、△はなくてもよい）
<table>
<tr><th>含むべき情報</th><th></th></tr>
<tr><td>TSAへのポリシーリンク</td><td>〇</td></tr>
<tr><td>時刻情報</td><td>〇</td></tr>
<tr><td>タイムスタンプ付与対象データのハッシュ値</td><td>〇</td></tr>
<tr><td>使用する公開鍵暗号技術の情報</td><td>〇</td></tr>
<tr><td>時刻精度</td><td>△</td></tr>
<tr><td>時刻ソース</td><td>△</td></tr>
<tr><td>発行者情報</td><td>△</td></tr>
<tr><td>検証のための情報</td><td></td></tr>
<tr><td>・公開鍵証明書またはその入手先情報</td><td>〇</td></tr>
<tr><td>有効期間</td><td>△</td></tr>
<tr><td>署名値</td><td>〇</td></tr>
</table></td><td>運用規程
タイムスタンプトークン</td></tr>
<tr><td>９　タイムスタンプトークンに含むべきでない情報</td><td>タイムスタンプトークンにはタイムスタンプの要求者の情報は含めないこと</td><td>運用規程
タイムスタンプトークン</td></tr>
<tr><td>10　非改ざん（完全性）を保証する情報</td><td>タイムスタンプトークンにトークン自体が改ざんされていないことを確認できる検知手段を施すこと</td><td>運用規程
タイムスタンプトークン
改ざん検知手段の説明資料</td></tr>
</table>

項目	基準（遵守事項）	エビデンス例
11　タイムスタンプトークンの生成に関わる暗号技術	タイムスタンプトークンの付与対象となる電子文書のハッシュ値を得るためのハッシュ関数、タイムスタンプトークンのデジタル署名に用いる公開鍵暗号技術は以下の条件を満たすものを使用すること	
1 電子文書のハッシュ値を得るためのハッシュ関数	タイムスタンプトークンの付与対象となる電子文書のハッシュ値を得るためのハッシュ関数は、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）（平成25年3月1日に総務省、経済産業省が公表したもの）において電子政府推奨暗号リストに記載されたハッシュ関数を用いること	運用規程 タイムスタンプトークン 安全性レベルの証明資料
2 タイムスタンプトークンのデジタル署名に用いる公開鍵暗号技術	タイムスタンプトークンの生成に関わる公開鍵暗号技術は、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）（平成25年3月1日に総務省、経済産業省が公表したもの）において電子政府推奨暗号リストに記載された公開鍵暗号技術を用いること。 ただし、署名に用いるRSAは2048ビット以上のビット長のものを使用すること、またRSAとは別の署名アルゴリズムを使用する場合はSHA256 with RSA 2048ビットと同等以上の安全性を持つものを使用すること。	運用規程 タイムスタンプトークン 安全性レベルの証明資料
12　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	タイムスタンプトークンの生成に使う秘密鍵は、HSM（FIPS140-2のレベル3認定相当以上の製品）を用いて保護する。	運用規程 TSU仕様書 HSM装置のカタログ、シリアルナンバー FIPS相当品使用の場合、相当することを示す十分な資料
13　タイムスタンプトークン生成に用いる秘密鍵に対する公開鍵証明書（TSA公開鍵証明書）	TSA証明書は、以下の要件を満たすものであること	
1 TSA用の公開鍵証明書であること	TSA用に発行された公開鍵証明書であること	TSA公開鍵証明書 当該証明書に係るCP／CPS
2 署名アルゴリズム	TSA公開鍵証明書およびそのルートCA証明書ならびに中間CA証明書(使用している場合)の署名アルゴリズムとして、電子政府における調達のために参照すべき暗号リスト(CRYPTREC暗号リスト）（平成25年3月1日に総務省、経済産業省が公表したもの）において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。 ただし、上記電子政府推奨暗号リストの署名アルゴリズムのうち、RSAについては2048ビット以上のビット長のものを使用すること、また同署名アルゴリズムのうちRSAとは別のアルゴリズムを使用する場合は、SHA256 with RSA 2048ビットと同等以上の安全性を持つこと。 注）なお、ルート証明書の署名アルゴリズムについては、当面の間、SHA-1の使用を認める。	TSA公開鍵証明書 当該証明書に係るCP/CPS
3 TSA公開鍵証明書の発行者の名称の記載	TSA公開鍵証明書に、その発行者の名称が記載されていること	TSA公開鍵証明書 当該証明書に係るCP/CPS
4 TSA公開鍵証明書の保持主体又は保持主体が行う業務の記載	TSA公開鍵証明書に、対応する秘密鍵の保持主体又は保持主体が行う業務の名称が記載されていること	TSA公開鍵証明書 当該証明書に係るCP/CPS
5 TSA公開鍵証明書の失効情報の記載	TSA公開鍵証明書の失効情報の公開ロケーションが記載されていること	タイムスタンプトークン TSA公開鍵証明書 CRL（Certification Revocation List)を公開する場所が書かれた資料
6 TSA公開鍵証明書有効期間の記載	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	TSA公開鍵証明書

項目	基準（遵守事項）	エビデンス例
7 TSA公開鍵証明書の正当性の確認	公開鍵証明書の正当性を示す情報を明らかにすること	TSA公開鍵証明書 ルートCAフィンガープリント
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	
1 TSA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監査を受けた認証事業者であること	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 TSA公開鍵証明書を発行する認証局との合意事項等	時刻認証事業者は、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。 ① 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 ② 認証局は、認証業務の終了後、秘密鍵を安全に廃棄し、その旨を書面にて時刻認証事業者に通知すること ③ 認証局が認証業務を他の認証局に引き継ぐ場合は、認証局の認証業務終了には当たらないものとし、引継ぎに先立ち、引継ぎ先の認証局と①、②と同様の合意を得ること （注）署名に用いる秘密鍵の取扱いについて運用基準9-5を参照のこと	CA秘密鍵の廃棄を証する廃棄証明書など 認証局との合意内容を証する書類
15 タイムスタンプトークンの生成処理	正しい時刻情報を含むタイムスタンプトークンの生成処理において、耐タンパー性を有する装置等で完全・正確なプログラムを実装していること	
1 当該プログラム等の完全性/正確性	時刻情報の取得からタイムスタンプトークンの生成に至るまでのプログラム等が正確に動作することを説明できること	事業者が行った当該プログラムの試験項目および試験結果 プログラムが正確に動作することについての説明資料（ブラックボックスの場合は、当該プログラムが認定制度の求める基準に合致していることを保証する製造ベンダーの宣言書等）
2 当該プログラム等の改ざんへの対策	当該プログラム等の改ざんを防止する仕組みを備え、検知した場合には検知の結果を記録すること	耐タンパー性を有する装置内で生成処理されている機能の説明資料および耐タンパー性を有する装置のセキュリティに関する説明資料（ブラックボックスの場合は、当該プログラムが認定制度の求める審査基準に合致していることを保証する製造ベンダーの宣言書等）
3 生成処理の実行の確認	タイムスタンプトークンの生成に係る正常なプロセスが動作していることおよび不要なプロセスが動作していないことを確認する仕組みを備え、不正な状態を検知した場合には検知の結果を記録すること	技術仕様書および実動作確認(例：動作しているプロセス名の確認および正常なプロセス名リストとの比較結果の記録等。ブラックボックスの場合は、当該プログラムが認定制度の求める基準に合致していることを保証する製造ベンダーの宣言書等）
16 タイムスタンプトークンの時刻の品質	タイムスタンプトークンの生成に用いる時刻の品質について以下の要件を満たすものであること	
1 正しい時刻情報	タイムスタンプトークン生成に利用する時刻情報は「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たものであることを説明できること	耐タンパー性を有する装置内で認定TAAから配信された時刻を用いて、生成処理されている機能の説明資料および耐タンパー性を有する装置のセキュリティに関する説明資料（ブラックボックスの場合は、当該プログラムが認定制度の求める審査基準に合致していることを保証する製造ベンダーの宣言書等）
2 時刻の品質の管理	TSAは（１）２項で定められた時刻精度を満たしていないタイムスタンプトークンの発行を防止するための措置を講じること 当該措置としてタイムスタンプトークンに含まれる時刻を外部の参照時計を用いて監視する場合、異常発生時には異常が明示され、また時刻差が記録されること	運用規程 システム構成概略図 処理フロー 時刻監視の仕組みと記録されるログについての説明資料

項目	基準（遵守事項）	エビデンス例
17　安全な検証手段の提供	TSA側で検証を行う場合、セキュリティ対策（なりすまし、改ざん、盗聴の対策、など）が行われた通信路上で検証者とタイムスタンプ検証サービス間の検証プロトコルを実行すること	IF仕様書
18　検証処理の要件	以下の要件を満たす適切な検証の手段を提供すること	
1 タイムスタンプトークンのデータ形式の崩れ、改ざんの判別	検証処理を行う者またはツールは、検証要求を受けたタイムスタンプトークンのデータ形式に崩れや改ざんがあることを判別できること	検証手段の仕様書 説明資料 デモ
2 TSA公開鍵証明書の有効性の判別	検証処理を行う者またはツールは、タイムスタンプトークンにTSA公開鍵証明書が含まれる場合、タイムスタンプトークン発行時におけるその証明書の有効性を検査できること	検証手段の仕様書 説明資料 デモ
	検証処理を行う者またはツールは、タイムスタンプトークンにTSA公開鍵証明書が含まれない場合、安全なリポジトリからタイムスタンプトークンのデジタル署名に用いられた証明書を取得し、検査できること	検証手段の仕様書 説明資料 デモ
	検証処理を行う者またはツールは、有効性を確認したTSA公開鍵を用いてタイムスタンプトークンに含まれるデジタル署名の有効性を検査できること	検証手段の仕様書 説明資料 デモ
3 タイムスタンプトークンからの改ざんの判別	タイムスタンプトークンが有効である場合、検証処理を行う者またはツールは、タイムスタンプトークンから元文書の改ざんが判別できること	検証手段の仕様書 説明資料 デモ

（２）運用基準

項目	基準（遵守事項）	エビデンス例
1　提供する業務の明確化	時刻認証事業者が提供する業務を明確に定め、以下の事項を含んでいること	
1 タイムスタンプトークンの生成・発行	利用者のリクエストに応じてタイムスタンプトークンを生成・発行すること	運用規程 サービス約款
2 時刻認証業務で使用する全ての時計の時刻管理	時刻認証業務で使用する全ての時計の時刻を十分な精度に維持すること	運用規程 サービス約款
3 時刻認証業務で使用する鍵の生成と管理	時刻認証業務で用いる暗号鍵を安全に生成し、管理すること	運用規程 サービス約款
4 時刻認証業務で使用する秘密鍵または暗号アルゴリズムが危殆化した場合の措置	時刻認証業務で使用する秘密鍵または暗号アルゴリズムの危殆化が発覚した場合は、速やかに当該秘密鍵または暗号アルゴリズムの使用を中止するとともに利用者に連絡すること	運用規程 サービス約款
	時刻認証業務で使用する秘密鍵とペアになる公開鍵について認証局から証明書の発行を受けている場合には、速やかに失効請求を行う義務を明示すること	運用規程 業務手順書
5 CAに対する通知	時刻認証業務を終了する時やTSA公開鍵証明書の記載事項の変更が有る場合、CAの定める方法によりCAに通知すること	運用規程 CAとの契約書類 CPS
6 検証手段の提供	検証者に対してタイムスタンプトークンの検証手段または検証に必要な情報を提供すること	運用規程 サービス約款

項目	基準（遵守事項）	エビデンス例
7 時刻認証業務で使用する暗号アルゴリズムの危殆化がタイムスタンプトークンの有効期間内に予想される場合の措置	時刻認証事業者は、タイムスタンプトークン生成に使用する暗号アルゴリズムの危殆化がタイムスタンプトークンの有効期間内に予測される事態になった場合に実施すべき次の対応策を策定しておくこと (a) 当該タイムスタンプトークンの発行停止予定日の決定と関係者への周知・報告 (b) TSA公開鍵証明書の失効予定日の確認と関係者への周知・報告 (c) 必要に応じて新たな暗号アルゴリズムを用いたサービスへ移行すること (d) タイムスタンプ更新により、その有効性が維持できることの関係者への周知・報告	運用規程 サービス約款
2 責任範囲の明確化	時刻認証事業者自身の責任と保証の範囲に関するポリシーを開示すること	
1 賠償責任	時刻認証事業者が負う賠償責任について開示すること	運用規程 サービス約款
2 免責事項	時刻認証事業者の免責事項について開示すること	運用規程 サービス約款
3 組織・人事管理	適切な組織構成および開発・運用維持、信頼性確保、可用性確保に対処できる能力・体制を確保すること	
1 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	組織図
2 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	担当部署の組織図 各役職の役割・要件の規定 教育訓練の記録または計画書
3 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	時刻認証に関する業務手順書 承認フロー（関係部分のみ）
4 業務監査	部署外からの業務監査等のチェック機能が働くこと	監査主体と事業担当部署の責任上独立が確認できる組織図
5 事故発生時処理	事故発生時に、その発生源が特定できること また、事故発生に対して適切な対応手順を定めておくこと	対応体制図 手順書（緊急連絡網、フロー図など） 障害対応手順書
6 事業継続計画	時刻認証業務を提供する事業者は、情報システムの重大な故障、自然災害、またはセキュリティ事故等の発生がタイムスタンプ利用者に大きな影響を与える可能性があることを認識して、最悪な事態を避けるためにも、タイムスタンプ利用者への影響を最小限に抑えた事業継続計画を策定し、事業継続に留意すること	事業継続に係る計画書または手順書
4 機密保持	セキュリティ維持にかかわる機密情報の保護、サービス利用者個人情報の保護について適切な措置を講じること	
1 セキュリティ維持にかかわる機密情報の保持	運用者の特定、運用体制、マシン室のレイアウト、監査情報、設備・システムセキュリティ等の機密情報については、その影響度を十分考慮した取扱い方法を定め、それに従った運用を行うこと	機密情報管理規定
2 利用者関連情報保護	利用者にかかわる情報が目的外に利用されたり、不正に漏洩されたりすることがないように、機密範囲とその取扱い方法を定め、それに従った運用を行うこと	個人情報管理規定
3 設備の物理的な隔離	利用者情報や監査情報、設備・システムセキュリティ等の機密情報を保護する保管設備については、施錠を行い物理的に隔離されていること	入退出管理手順 保管場所

項目	基準（遵守事項）	エビデンス例
5　業務の一時停止・終了	業務一時停止・終了時の利用者への事前通知等の手順が明確に定められていること	
1 事前通知	サービスの一時停止・終了時は、事前にそのスケジュールと手続きを決め、その内容を事前に公知、もしくは利用者へ通知すること	運用規程 サービス約款
2 サービス終了時の移行期間の確保	サービスを終了する際は、利用者が新たな時刻認証業務へ移行するために十分な移行期間を確保すること	運用規程 サービス約款
3 予告なしの業務停止の禁止	障害発生時などの予期できない場合の緊急停止措置以外は、事前の通知なしに業務を一時停止しないこと	運用規程
6　業務監査	時刻認証業務の適切な運用をチェックするため、定期的に部署外からの適切な業務監査を受け、その結果を認定機関へ開示すること	
1 監査内容	時刻認証業務が本審査基準に沿って適切に実施されていることを確認する業務監査を計画し、実施すること	監査実施要綱 監査計画書
2 監査情報の保管	保管すべき監査情報と保管期間を定めること	監査実施要綱
	保管に当たってはアクセス権限を明確にし、不正アクセスによる情報の改ざん、消去、漏洩等の防止策を講じること	監査実施要綱 監査情報保管環境の説明資料
3 監査の頻度	監査の頻度は、最低年１回実施すること	監査実施要綱 監査結果報告書（初回はなし）
4 監査結果の認定機関への開示と対処情報	監査実施後は、認定機関に対して監査結果を速やかに開示するものとし、監査の結果として欠陥が指摘された場合には、以下要件を速やかに対処すること １．欠陥が修正されるまでの対処 （例えば、運用の停止、利用者に対する十分なアナウンス等） ２．指摘された欠陥への対処	監査実施要綱 監査結果報告書（初回はなし） 監査指摘事項への対処計画または結果
7　時刻認証業務の運用に関する記録の取得と保管	時刻認証業務の運用に関する重要な事象およびデータを記録すること、また、記録は全て期間を決めて保管すること	
1 記録する情報の明文化と保管期間	記録する情報対象はその保管期間とともに、文書化しておくこと	運用規程
2 記録する情報の安全な保管と可用性確保	記録する情報は、完全性と機密性を保つとともに必要に応じて利用できるように保管すること	運用規程
3 記録する情報	記録する情報は、本審査基準で保管が求められているものに加えて下記を含むこと a) 時刻配信局より受けた時刻監査記録(または時刻監査証明書のコピー) b) タイムスタンプトークン生成に使用する鍵ペアの生成・失効記録ならびに秘密鍵廃棄の記録 c) 時刻認証業務にかかわるシステムの動作異常の記録	運用規程
8　システムのトラブル、破壊からの復旧	システムトラブルやシステムの破壊等に対して、緊急停止手段やバックアップデータによる復旧手段を用意すること	
1 時計システムのトラブル対処	時刻認証業務で使用する時計システムの時刻精度が運用規程の規定範囲外になった場合は、システムトラブルとみなし、システムの緊急停止および復旧作業を速やかに行うこと	障害対応手順書
2 ハードウェア、ソフトウェアまたはデータが破壊された場合の対処	バックアップ用のハードウェア、ソフトウェアまたはデータにより速やかに復旧作業を行うこと	障害対応手順書

項目	基準（遵守事項）	エビデンス例
9　タイムスタンプトークン生成に用いる秘密鍵の管理	タイムスタンプトークン生成に用いる秘密鍵とそれに対応する公開鍵証明書を安全に管理すること	
1 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、複数人管理のもとで行うこと	運用規程 業務手順書
2 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（FIPS140-2のレベル3認定相当以上の製品）内に保管すること	運用規程 使用するHSMの仕様書
	複数人の権限を有する者が揃わなければ、HSM（FIPS140-2のレベル3認定相当以上の製品）の持ち出し等ができないよう、複数人管理のもとで保管すること	運用規程 業務手順書
	秘密鍵のバックアップは行わないこと 秘密鍵のバックアップが可能な場合は、当該の機能を利用できない設定にしておくこと	運用規程
3 鍵の利用	保管されている秘密鍵を用いてデジタル署名する際には、HSM（FIPS140-2のレベル3認定相当以上の製品）内部で安全に処理すること	HSM内で署名処理されている機能の説明資料
	HSM（FIPS140-2のレベル3認定相当以上の製品）をタイムスタンプトークン生成システム等に接続したり、HSM（FIPS140-2のレベル3認定相当以上の製品）内の鍵を利用可能状態にする操作は、複数人管理のもとで行うこと	運用規程
4 TSA公開鍵証明書の保存	TSA公開鍵証明書は有効期間満了後も可用性を確保することが必要であり、改ざんされないように保存すること	運用規程
5 鍵の廃棄	必要な期間が終了した鍵や、失効した鍵、危殆化した鍵などは、その後の不正利用が行われないように廃棄すること また、認証局が認証業務を終了する場合、認証局の業務終了までに当該認証局の発行に係るTSA公開鍵証明書に対応する秘密鍵を安全に廃棄すること	運用規程 業務手順書 TSA秘密鍵の廃棄を証する廃棄証明書など
	廃棄は、複数人管理のもとで、秘密情報の一部でも露顕したり残存させたりすることなく行われること	運用規程 業務手順書
6 鍵の更新	新しいTSA公開鍵証明書を用いたタイムスタンプトークンの発行サービスを開始するときには、TSA公開鍵証明書が正当なものであることを確認し、更新後のサービス開始前にタイムスタンプットークンが正当なものであることを確認すること	運用規程 業務手順書
	タイムスタンプトークン生成に用いる秘密鍵は、あらかじめ有効期間と活性化期間を設け定期的に更新すること 更新期間は時刻認証業務のポリシーで適切に定めること	運用規程 業務手順書
	鍵の有効期間および活性化期間は、タイムスタンプトークン付与対象の電子文書のハッシュ値を得るためのハッシュ関数およびタイムスタンプトークンの生成に用いる公開鍵暗号技術の最新の安全性評価情報を元に決定すること	運用規程 業務手順書
7 鍵の危殆化時の対応	時刻認証事業者は、タイムスタンプトークン生成に用いる秘密鍵が内部不正によって漏洩したり、第三者によって秘密鍵が解読された場合に備えて、あらかじめ対応策を策定しておくこと	運用規程 危殆化対応手順書
	タイムスタンプトークン生成に用いる秘密鍵の危殆化が発覚した場合、当該秘密鍵が危殆化したこと、および対応するTSA公開鍵証明書を失効させたことをサービス利用者に速やかに通知、もしくは情報公開すること	運用規程 危殆化対応手順書
10　タイムスタンプトークン生成を行うプログラムの変更および操作	当該プログラムの変更、操作をするときは、以下の要件を満たすこと	

項目	基準（遵守事項）	エビデンス例
1 当該プログラムの変更	当該プログラムへ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	運用手順書
2 当該プログラムの操作	当該プログラムの設定に関する操作は複数人管理で行うこと	運用手順書
11 通信に用いる暗号鍵の管理	TAAとの通信路の安全性を公開鍵暗号技術または共通鍵暗号技術により実現する場合、それらの暗号鍵を安全に管理すること	
1 鍵の生成	鍵の生成は、信頼できる鍵生成システムを利用し、複数人管理のもとで行うこと	運用規程 業務手順書
2 鍵の保管	通信に用いる秘密鍵または共通鍵は、十分なセキュリティが確保できる環境で保管すること	運用規程 業務手順書
3 有効期間	通信に用いる暗号鍵は、用いる暗号技術の最新の安全性評価を元に、適切な有効期間を設けること	運用規程 業務手順書
4 鍵の廃棄	有効期間が経過した鍵や、失効した鍵、危殆化した鍵などは、その後の不正利用が行われないように廃棄すること	運用規程 業務手順書
12 タイムスタンプトークンの有効期間	タイムスタンプトークンの有効期間を適切に定め、利用者に通知すること	
1 タイムスタンプトークンの有効期間の設定と通知	タイムスタンプトークン生成に用いる暗号技術から保証される当該タイムスタンプトークンの有効期間と、あらかじめ定めた活性化期間をもとにタイムスタンプトークンの有効期間を適切に定め、利用者に通知すること	運用規程 タイムスタンプトークン
2 有効期間の短縮の可能性の通知	タイムスタンプトークンの有効期間を利用者に通知する際には、タイムスタンプトークンの生成に用いる秘密鍵または暗号アルゴリズムの安全性評価や危殆化等によって、タイムスタンプトークンの有効期間が短縮される可能性があることを明確に伝えること	運用規程 タイムスタンプトークン

（３）ファシリティの基準

項目	基準（遵守事項）	エビデンス例
1 耐震基準		
1 建築物の耐震性	時刻認証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	確認通知書 検査通知書 地盤調査書
2 設備の耐震性	時刻認証業務用設備は通常想定される規模の地震による転倒や構成部品の脱落などを防止するための構成部品の固定その他の耐震措置が講じられていること	レイアウト図
2 耐火基準	時刻認証業務に係る設備を含む建築物は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	確認通知書 検査通知書
3 水害防止	水害の防止のための措置が講じられていること	システムの物理的配置を説明する書類
4 電気設備	ビルの電源検査時に無停電で行えること、緊急災害時に業務の継続を確保できるレベルの無停電電源装置、バックアップ発電機などの瞬停対策があること	機器説明書などの確認資料 災害時運用手順書 レイアウト図面
5 火災報知システム	自動火災報知機および消火装置が設置されていること	消防用設備等検査済証等
6 空調設備	時刻認証業務を行うための性能を維持できる温湿度管理がされていること	温湿度管理ポリシー
7 認定対象設備に対するアクセス		

項目	基準（遵守事項）	エビデンス例
１ 認定対象設備	時刻認証業務に係るシステム全体を権限ある者のみが開錠可能な別室または錠付きラックにて囲い安全性を確保すること	レイアウト図面 入退室管理の手順書
２ 入退室管理	時刻認証業務に係るシステム全体のある部屋およびオペレーションルームの入退室の管理を実施すること 例　バイオメトリックスシステム、ICカードシステムなど	入退室管理手順書

（４）システム安全性の基準

項目	基準（遵守事項）	エビデンス例
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	システム構成図 セキュリティに関する更新履歴
２　内部ネットワーク（ＬＡＮ）	サービスもしくは機能ごとに、サーバ等機器を適切に配置し、不要な通信を遮断できるようにすること（例：レイヤー3スイッチによる分離） ネットワーク機器は必要に応じてセキュリティ更新がなされること	システム構成図 ポートの設定情報 セキュリティに関する更新履歴
３　サーバ・ストレージ		
１ サーバ機能の設定	時刻認証業務にかかる全てのサーバ機能の設定は適切に行うこと（例：不要アクセスの拒否、不要アプリケーション削除、不要ポートの利用停止など）	機能設定確認書
２ セキュリティの運用管理	業務に係る全てのサーバについて適切な運用管理を行うこと（例：十分なテストをした上でのセキュリティパッチ対応、ファイルの整合性の確認、システムログの記録など）	運用手順書
４　システムの可用性	時刻認証業務に係るシステムの障害に備えて、サービスを継続するための対策を実施していること	システム構成図
５　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が取れていること	システム運用手順書 時刻同期方法の説明資料

（５）情報開示の基準

項目	基準（遵守事項）	エビデンス例
１　TSAポリシーの公開	以下の内容を含む運用規程を定め、随時参照可能にしておくこと	
１ 事業者情報	事業者名、住所、問い合わせ窓口情報（電話、e-mailアドレス等）を明記	運用規程
２ 保持している時刻源（時計）とUTCとの最大時刻差	時刻認証業務で使用する時刻ソースの特定情報（OID等）を明記 運用上の確保可能な最大時刻差情報を明記	運用規程
３ 時刻監査情報	時刻監査証、監査記録の開示方法を明記（タイムスタンプトークンに時刻監査証または監査記録を含まない場合）	運用規程
４ TAAとのポリシーリンク	時刻認証業務で時刻配信・時刻監査を受けるTAAとのポリシーリンクをOID、URL等により明記	運用規程
５ サービス内容と事業者の義務	時刻認証業務の提供において事業者が提供するサービス内容と事業者が負う義務を明記	運用規程
６ 事業者の責任範囲	時刻認証業務の提供に関して事業者が負う賠償責任の範囲と免責事項を明記	運用規程
７ 技術情報	時刻認証業務の安全性や信頼性を判断できる技術情報を明記	運用規程

項目	基準（遵守事項）	エビデンス例
8 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記	運用規程
9 タイムスタンプトークンに含まれる時刻情報の時系	タイムスタンプトークンに含まれる時刻情報の時系を明記	運用規程
10 暗号アルゴリズムに関する情報	時刻認証業務で使用する暗号アルゴリズムに関して、下記の情報を明記 ・タイムスタンプトークンに用いる暗号アルゴリズム（電子文書のハッシュ関数およびデジタル署名に用いる公開鍵暗号技術） ・暗号アルゴリズムが危殆化した場合の対応策 ・暗号アルゴリズムの危殆化がタイムスタンプトークンの有効期間内に予測される場合の対応策	運用規程
11 タイムスタンプトークンの有効期間	ハッシュアルゴリズム、署名生成鍵の鍵長から保証される署名の有効期間、活性化期間、タイムスタンプトークンの有効期間を明記	運用規程
	タイムスタンプトークン生成に用いる暗号アルゴリズムの安全性評価や危殆化等によって、設定した有効期間が短縮される可能性があることを明記	運用規程
12 検証のための情報	タイムスタンプトークンの検証に必要な情報を明記 ・TSA公開鍵証明書の入手方法 ・検証の方法（検証手順、ツール等）の情報	運用規程
13 運用規定	事業者が規定する運用規定を明記	運用規程
14 サービス時間帯	サービスを提供する時間帯を明記	運用規程
15 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 サービス利用に関わる注意事項があれば明記	運用規程
16 利用者個人情報、機密情報に関する取り扱い	情報の取得、管理、保存期間、廃棄、開示に関わる要件を明記	運用規程
17 サービス一時停止・終了時の対応	サービス一時停止・終了時に事業者がとる対応と利用者への通知について明記	運用規程
18 暗号鍵の管理	タイムスタンプトークン生成に用いる暗号鍵の管理、更新期間、危殆化発覚時の対応について明記	運用規程
19 システムトラブル等の発生時の対応	システムトラブル、システム破壊、災害発生時に事業者がとる対応と利用者への通知について明記	運用規程
20 準拠法	日本国内法および規制に基づき解釈されることを明記	運用規程
2　利用者および利用者に関わる関係者への情報開示	利用者および利用者に関わる関係者に対して、運用規程の情報公開に加えて、必要に応じて以下の情報を開示すること	
1 問い合わせ情報	利用者用の問い合わせ窓口情報（電話、e-mailアドレス等）	利用者、検証者向け説明資料
2 時刻監査情報	時刻監査証、監査記録	タイムスタンプトークン リポジトリ
3 TSA公開鍵証明書の有効期間	デジタル署名に公開鍵暗号基盤を用いる場合は、TSA公開鍵証明書の有効期間の情報を明記	TSA公開鍵証明書
4 TSA公開鍵証明書の失効に関する情報	デジタル署名に公開鍵暗号基盤を用いる場合は、TSA公開鍵証明書の失効リストの公開ロケーションを明記	TSA公開鍵証明書 リポジトリ

項目	基準（遵守事項）	エビデンス例
5 検証のための情報	タイムスタンプトークンの検証のための情報 ・TSA公開鍵証明書 ・検証の方法（検証手順、ツール等）	タイムスタンプトークン リポジトリ
6 時刻認証サービス利用に関わる注意事項	運用規程記載以外の注意事項があれば明記	
	・タイムスタンプトークンの有効期限とタイムスタンプ付与対象文書の保存期間との関係について明確に注意喚起すること	利用者、検証者向け説明資料
	・タイムスタンプトークン生成に用いる暗号アルゴリズムおよび有効期間の設定と、電子政府推奨暗号リストとの関係について明記	利用者、検証者向け説明資料
	・本認定は、有効期間を経過したタイムスタンプトークンの信頼・安心を裏付けるものではないことを明記	利用者、検証者向け説明資料
	・タイムスタンプトークン生成に用いる暗号アルゴリズムの安全性評価や危殆化等によって、タイムスタンプトークンの有効期間が短縮される可能性があることを明記	利用者、検証者向け説明資料
	・タイムスタンプトークン生成に用いる暗号アルゴリズムの危殆化が生じた場合に時刻認証事業者が取る対策（当該暗号アルゴリズムを用いたタイムスタンプトークンの発行停止、TSA公開鍵証明書の失効、利用者への周知、新サービスへの移行など）を明記	利用者、検証者向け説明資料
7 利用者個人情報、機密情報等に関しての取扱い	利用者個人情報の開示請求手続き等の情報	利用者、検証者向け説明資料 事業者のWebサイト
3 利用者への通知・連絡	以下の場合には、速やかに利用者へ通知・連絡するように努めること	
1 サービス一時停止・終了時の通知	サービス一時停止・終了時には事前に利用者へ通知すること	通知文書など
2 秘密鍵または暗号アルゴリズムの危殆化時の通知	時刻認証業務に用いる秘密鍵または暗号アルゴリズムの危殆化の発覚時、あるいは暗号アルゴリズムの危殆化が有効期間内に予測される場合には、対応するTSA公開鍵証明書の失効等について速やかに利用者に通知すること	通知文書など
3 システムトラブル等の発生時の通知	システムトラブル、システム破壊、災害発生時には障害の発生と復旧見通しについて速やかに利用者に通知すること	通知文書など
4 開示情報の変更連絡	運用規程や利用者に開示する情報の内容に変更があった場合には、速やかに利用者へ連絡すること	連絡文書など